CHIP

CHIP PROFESSIONELL

Mit DVD

€ 19,95
Österreich, Luxemburg: € 19,95
Schweiz: sfr 30

AUSGABE 02/2005
MÄRZ / APRIL

4 196592 519955 02

Autoren dieser Ausgabe: Stefan Bönsch, Andreas Bröhl, Michael Coci, Hans Franzl, Christian Gauer, Martin Goldmann, Dr. Ralf Hinkel, Peter Klau, Bernhard Knaus, Martin Kuppinger, Robert Schoblick, Florian Schuster, Prof. Dr. Axel Sikora, Thomas Vosseberg, Stefan Wischner

Wireless professionell

So konfigurieren & sichern Profis W-LANs

Die Praxis-Referenz: Vom optimalen Heimnetzwerk bis zu Richtfunk-Netzen

WiFi, Bluetooth, RFID, WiMAX, Blackberry

Know-how für morgen: Welche Wireless-Standards & Techniken Zukunft haben

Exklusiv: Top-Tipps der Wireless-Experten

Wie Admins W-LANs tunen, absichern und Probleme lösen

SPECIAL: Neue Sicherheit für drahtlose Netze

Gefahren-Analyse und Strategien gegen Hacker & Malware

Experten-Wissen für die tägliche Praxis

Site Survey, professionelle Hotspots, Wireless Bridges, vermaschte Funknetze, drahtloses Home-Entertainment, ZigBee-Standard, Tipps & Troubleshooting

AUF DVD

VOLLVERSION **Intranator Enterprise-Edition**
Security Gateway mit Mailserver und Firewall

VOLLVERSION **Back Protection 2004**
Schützt Daten vor Zugriff aus LAN, Web, Spyware

VOLLVERSION **Ace Backup 2003**
Komprimierte und verschlüsselte Backups

Plus 360 Wireless-Tools

AirCrack WEP-Key-Test, **AiroPeek SE** Site-Survey-Tool, **AirSnare** MAC-Überwachung, **Cqure AP** Mini-AP, **FakeAP** W-LAN tarnen, **KisMAC** Apple-Sniffer, **Kismet** Linux-Sniffer, **NetStumbler** Windows-Sniffer, **PHLAK** Security-Linux, **WiFiFoFum** PocketPC-Sniffer, **WLAN Expert** Netz optimieren

Die DVD enthält keine jugendbeeinträchtigenden Inhalte.

THOMAS H. KASPAR, CHEFREDAKTEUR CHIP-SONDERHEFTE

Guter Inhalt zählt auch heute etwas

Zum Start von CHIP Professionell vor fast einem Jahr haben uns viele für verrückt erklärt: Ein Heft ohne bunte Bildchen, vollgestopft mit Text. Ein puristischer Titel, der auf jeden Schnickschnack verzichtet und sich komplett auf das konzentriert, wofür CHIP Professionell steht: Hochwertige Beiträge von hochqualifizierten Autoren.

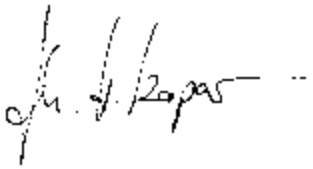
→ CHIP PROFESSIONELL STEHT FÜR WICHTIGE THEMEN – STIMMEN SIE AB!
Ich nehme mir die Freiheit, in dieser Reihe auch Themen zu realisieren, die in vielen anderen Heften keinen Platz mehr finden. Wahrscheinlich werden Sie jetzt nicht gleich Mesh-Netze aufbauen oder ZigBee einsetzen. Doch was Prof. Dr. Sikora darüber zu sagen hat, ist schlichtweg faszinierend und zeigt, wie Wireless-Technologien unser Leben morgen maßgeblich mitbestimmen. Unsere regelmäßige Leserbefragung (diesmal auf 13) zeigt, dass wir auf 148 Seiten ausreichend Nutzwert bieten: Das gibt uns den Spielraum, auch Nebenäste am großen Baum des Mainstream zu pflegen.

→ CHIP PROFESSIONELL IST EIN NETZWERK – SIE GEHÖREN DAZU!
Von der ersten Ausgabe an war CHIP Professionell eine Community. Ein neues Buch zu einem Trend: Könnte der Autor nicht auch für uns schreiben? Wie sehen Profis den IT-Alltag – wie können wir sie dafür gewinnen, ungewöhnliche Tipps zu geben, die im Alltag weiterhelfen? Welche Universität ist anderen bei einem Thema weit voraus – welche Experten könnten für unser Heft schreiben? Und natürlich: Was denken die Leser? Dazu diskutieren wir in den CHIP-Foren, leiten Anfragen an die Experten weiter oder besorgen einfach nur zusätzliche Listings.

→ CHIP PROFESSIONELL KOSTET VIEL GELD – FORDERN SIE UNS!
Die beiden größten Verrücktheiten zum Schluss. Die erste: Um hochwertige Artikel bringen zu können, verlangen wir für eine Ausgabe den Hammerpreis von knapp 20 Euro. Und wir bieten das Heft im Abo für 99 Euro im Jahr an (Infos auf 113). Doch in Windeseile hatten wir genügend Leser, die diese Art der Information schätzen.

Dafür beging ich die zweite Verrücktheit: Ich stehe mit persönlicher E-Mail und Telefonnummer für meine Hefte gerade. „Du wirst dich wundern“, unkten Kollegen. Wer glaubte, dass die Chefredakteurs-Nummer zur Support-Hotline verkommt, wurde enttäuscht: Kluge Anfragen, Themenvorschläge und Bitten um vertiefte Infos. Ich habe viel dazugelernt. In jedem Fall konnten wir helfen. CHIP Professionell-Leser sind eben anders. Schön, für solche Menschen schreiben zu dürfen.

Viel Spaß beim Vernetzen!



Thomas H. Kaspar, CHIP Professionell
tkaspar@chip.de, 089/746 42 527

3 Vollversionen, 360 aktuelle Tools

Die CHIP-Wireless-Toolbox für W-LAN-Admins: Eine DVD mit mehr als 360 der besten Tools für drahtlose Netze in der neuesten Version – bewährte Freeware, Shareware und Trials. Dazu drei Vollversionen.

Profi-Tools für Zugangs-Kontrolle und Monitoring

Aktuelle Trials von Aegis Client, Airmagnet Laptop Analyzer, Airopeek SE, LinkFerret Network Monitor.

Geniale Blackberry-Software für unterwegs

Mobil arbeiten mit eOffice, sichere Verschlüsselung mit CryptMagic, überall ins Web mit dem Webviewer.

Vollversion: Ace Backup 2003

Lassen Sie wichtige Daten vollautomatisch und platzsparend sichern. Dank Verschlüsselung unknackbar.

Vollversion: Intranator Enterprise-Edition

Gemeinsamer Internet-Zugang, Fax- und Mail-Server, VPN, Firewall, Anti-Viren-Tool, Inhaltskontrolle per Proxy-Server.

Gratis: W-LAN prüfen und optimieren

Der WLAN Expert zeigt Fehler und Störquellen im drahtlosen Netz an und ermittelt die Signalqualität.

W-LAN-Analyse und Schutz unter Linux

Top-Freeware für Linux: Drahtlose Netze aufspüren mit den Sniffern Kismet und WellenReiter, WEP-Schlüssel auf Sicherheit testen mit AirSnort.

AKTUELL

6 **CeBIT-Vorschau: Neue Wireless-Produkte**
Das sind die Neuigkeiten, mit denen die größte Computer-Messe der Welt zum Thema Wireless aufwarten kann.

8 **„Alle mobilen Geräte werden W-LAN-fähig“**
CHIP sprach mit Ulrich Gobbers, Entwicklungschef von Terratec, und Kathrin Posnanski, Marktforscherin beim DPM-Team, über Audio-Streaming fürs Wohnzimmer und den Höhenflug von O2.

36 **DVD-Highlights mit CHIP-Tipps**
Auf vier Seiten präsentiert CHIP insgesamt 22 Highlights der Heft-DVD mit zusätzlichen Tipps zu jedem Programm.

KNOW-HOW

14 **Wireless – die Zukunft ist drahtlos**
Was hinter der Wireless-Technik steckt und nach welchen Kriterien drahtlose Netzwerke funktionieren.

20 **TCP/IP konfigurieren**
So richten Sie das TCP/IP-Protokoll ein, damit die Computer im W-LAN kommunizieren können.

22 **So funktioniert das mobile Büro**
Die richtige Hardware für das mobile Büro: Woran Geschäftsreisende denken sollten.

26 **Leben und arbeiten mit WiFi**
Der Standard Wireless Fidelity (WiFi) ermöglicht Notebooks und Handhelds den drahtlosen Internet-Zugang.

28 **Funknetz mit Bluetooth**
Bluetooth ist ideal für temporäre drahtlose Vernetzungen im Nahbereich - auch mit Handys, Druckern und PDAs.

32 **Blackberry – immer per Mail erreichbar**
E-Mails sofort nach ihrem Eintreffen im Firmennetz auf dem Handheld lesen - Blackberry macht's möglich.

40 **WiMAX – das Super-W-LAN**
Die zukünftige Breitband-Technik WiMAX soll mit 75 MBit/s bis zu 50 Kilometer weit funken - 250fache W-LAN-Reichweite.

42 **Das Potenzial von RFID**
Die Radio Frequency Identification (RFID) muss mit vielen Vorbehalten kämpfen. Kommt jetzt der gläserne Kunde?

W-LAN AUFBAUEN

44 **Hardware für das Funknetzwerk**
In diesem Beitrag erfahren Sie alles über Access Points, W-LAN-Karten und weitere wichtige Hardware.

50 **Die richtige Antenne kaufen**
Wer die Reichweite seines Funknetzes erhöhen will, sollte sich eine externe Antenne zulegen. CHIP hilft beim Kauf.

52 **So geht's: W-LAN unter XP einrichten**
In wenigen Schritten konfigurieren Sie Ihr drahtloses Netzwerk unter Windows XP.

58 **Netz-Ressourcen freigeben**
So richten Sie Datei- und Drucker-Freigaben in Ihrem W-LAN ein, ohne dass dabei die Sicherheit zu kurz kommt.

62 **Kabellos zuhause arbeiten**
Surfen und arbeiten in den eigenen vier Wänden - so richten Sie sich ein Wireless Home Office ein.

64 **W-LAN unter Linux mit SuSE aufbauen**
Mit SuSE LInux 9.2 ist die Konfiguration eines W-LAN keine Geheimwissenschaft mehr. CHIP hilft beim Einrichten.

Aufbau-Spezialist

Peter Klau, Programmierer und Netzwerkverwalter, arbeitet seit etwa 15 Jahren als IT-Journalist und Buchautor. Er schrieb die meisten Beiträge in den Rubriken „Know-how“ und „Aufbau“.

Mesh & ZigBee

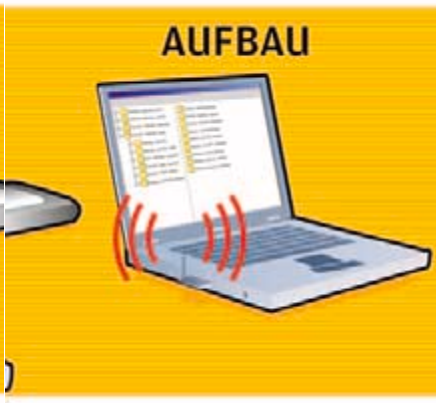
Prof. Dr. Axel Sikora ist Fachleiter Informationstechnik an der Berufsakademie Lörrach. Der Diplom-Ingenieur verfasste die Beiträge über die neuen drahtlosen Topologien und Standards ab 114.

Drahtloser Linux-Fan

Martin Goldmann, Journalist, Buchautor und bekennender Linux-User, verrät Ihnen ab 64, wie Sie mit SuSE Linux 9.2 ein drahtloses Netzwerk aufbauen.

Netzwerk-Wächter

Michael Coci ist Product Marketing and Support Director für EMEA bei Trapeze Networks. Wie er Eindringlinge im Netzwerk stellt, lesen Sie in den Experten-Tipps auf 79.



TK-Fachmann

Robert Schoblick, seit 1991 freier Journalist, beschäftigt sich schon lange mit TK- und IT-Themen. Von ihm stammen die meisten Artikel aus der Rubrik „Praxis“.

Sicherheits-Profi

Thomas Vosseberg ist Sicherheitsberater bei der mns-security und schult System-Administratoren. Von ihm stammt das Sicherheits-Special ab 68 in dieser Ausgabe.

Vernetzte Kameras

Dr. Ralf Hinkel ist Vorstand der Mobotix AG, die wetterfeste Netzwerk-IP-Kameras produziert. Er schrieb die Experten-Tipps zur digitalen Videoüberwachung auf 95.

Planungs-Experte

Christian Gauer ist Leiter Technik beim IT-Lösungsanbieter DDS GmbH in München. Er schrieb die Experten-Tipps zum Thema Site Survey auf 99.

SPECIAL

Sicherheit in drahtlosen Netzen 68
Hacker, Sniffer, War-Driver – ein W-LAN steht oft unter Beschuss. CHIP sagt Ihnen, mit welchen Gefahren Sie rechnen müssen.

Wireless LAN perfekt abschirmen 76
Mit cleveren Sicherheitsstrategien schotten Sie Ihr Funknetz rigoros ab und bringen die Hacker um ihr Erfolgserlebnis.

Die besten Tipps & Tricks für mehr Sicherheit 80
So schützen Sie Ihr drahtloses Netzwerk vor War-Drivern und neugierigen Büronachbarn.

Computerrecht: Schwarzsurfer im W-LAN 83
Aufgepasst: Wenn ungebetene Gäste in Ihrem Funknetz auf Ihre Kosten surfen, handeln sie oft noch nicht einmal strafbar.

PRAXIS

Home-Entertainment per W-LAN 84
Filme anschauen, Musik hören, im Web surfen – und das überall im Haus. Ein Home-Entertainment-Netz machts möglich.

Optische Raumüberwachung 92
Wie Sie eine drahtlose Video-Überwachungsanlage aufbauen und in Betrieb halten, erfahren Sie in diesem Beitrag.

Site Survey: Große Funknetze richtig planen 96
Wer ein professionelles W-LAN mit großer Reichweite aufbauen will, sollte zuvor das Funkareal auf Störeinflüsse prüfen.

So geht's: Professionellen Hotspot einrichten 102
Ein Hotspot ist auch für kleinere Unternehmen ein attraktiver Kunden-Service. CHIP unterstützt Sie bei der Planung.

Wireless Bridges: W-LAN statt Festnetz 110
Für Distanzen von bis zu fünf Kilometern Luftlinie bietet die W-LAN-Technik eine gute Alternative zum Kabel.

Vermaschte Funknetze: Mesh-Netze mit W-LAN 114
Wenn der Access Point zur Bridge wird – vermaschte Netz-Topologien können die Grundlage für ganze Stadtnetze bilden.

Neuer Funk-Standard: Vernetzen mit ZigBee 118
Im Nahbereich lassen sich mit ZigBee Messaufnehmer, Schalter, Motoren oder Lampen vernetzen – äußerst preisgünstig.

Netzwerkstatus überwachen 122
Mit verschiedenen Windows-Tools können Sie Ihr Funknetzwerk bei der Arbeit genau im Auge behalten.

Strategische Fehlersuche im W-LAN 128
Wie Sie die häufigsten Fehlfunktionen im Funknetzwerk aufdecken und erfolgreich abstellen, zeigt Ihnen dieser Beitrag.

Perfekt funken: W-LAN-Tipps für Profis 134
Wie Sie geheime Firmware aufspielen oder eine W-LAN-Antenne bauen, erfahren Sie in unseren exklusiven Profi-Tipps.

Tuning fürs Funknetz: Funknetz voll ausreizen 139
Musik & Video, Drucker, Fileserver, Fernseher – mit diesen Tipps gibt's beim drahtlosen Vernetzen keine Probleme mehr.

Tipps & Troubleshooting 142
Für den Fall, dass es mal klemmt im Funknetz: CHIP hat für Sie die besten Tipps und Hilfen zur Problemlösung bereitgestellt.

RUBRIKEN

Leser-Umfrage 13
Impressum 146
Vorschau 146

Die besten Sicherheits-Tools für Wireless LAN

W-LAN auf Lücken testen mit Top-Freeware wie Aerosol, kostenloser LAN Schutz z.B. mit AirSnare.

Kostenlos: Geniale Site Survey Software

Der NetStumbler findet und analysiert drahtlose Netzwerke und gibt Aufschluss über Signalstärke und Verschlüsselung.

BSI-Broschüre: Sicherheit im Funk-LAN

Der offizielle Leitfaden des Bundesamtes zeigt Risiken im W-LAN und erklärt geeignete Schutzmaßnahmen.

Die beste Software für LAN-Administration

Top-Tools wie der Packet-Sniffer Ethereal, das Monitoring-Tool Look@LAN, NetSetMan oder der Portscanner NmapWin.

Vollversion: Back Protection 2004

Wichtige Daten vor Fremd-Zugriff über Netz, Web oder Spyware schützen, verschlüsselte Kommunikation.

Top-Analyse-Tools für Ihr Wireless LAN

Sniffer wie AirTraf, Mognet, MiniStumbler, KisMAC oder iStumbler, Netzwerk-Schutz mit FakeAP und AP-Utils.

Filme über drahtlose Netzwerke streamen

Der VideoLAN Client ermöglicht es, Fernsehen, Video- und Sound-Dateien über ein (W-)LAN zu streamen. So hat jeder Rechner im Netzwerk zentralen Zugriff auf alle Medien.

Mitmachen und gewinnen!

Sagen Sie uns Ihre Meinung zu diesem Heft und gewinnen Sie einen der attraktiven Preise.

Drahtlose Netzwerke 2005

Mit Sicherheit schneller

Während im vergangenen Jahr vor allem die Jagd nach höherer Datenrate die Wireless-Welt prägte, gilt 2005: Sicherheit geht vor. Für dieses Jahr kündigen die Hersteller eine Vielzahl neuer W-LAN- und Bluetooth-Geräte samt raffinierten Verschlüsselungs-Techniken an und versprechen – ganz nebenbei – bis zu sechsmal höhere Datenraten.

Drahtlose Vernetzung ist einer der ganz großen IT-Trends auf der diesjährigen CeBIT. Neben einer hohen Übertragungsgeschwindigkeit sind bei neuen Produkten vor allem effiziente Absicherungsmechanismen gefragt. Atheros und D-Link etwa arbeiten an „JumpStart“, einem Konzept, das eine höchstmögliche Sicherheit in wenigen Mausklicks verspricht. Broadcom, Linksys und HP verfolgen mit „SecureEasySetup“ ein ähnliches Ziel. In punkto Übertragungsgeschwindigkeit markieren im Consumer-Bereich derzeit 108 MBit/s das theoretische Maximum, im nächsten Jahr sollen über 600 MBit/s erreicht werden. Als Grundlage für derart hohe Datenraten dient IEEE 802.11n mit einer standardisierten MIMO-OFDM-Technik (Multiple Input Multiple Output Orthogonal Frequency Division Multiplexing). Dem Vernehmen nach wird IEEE 802.11n allerdings nicht vor Mitte nächsten Jahres verabschiedet. UTStarcom kombiniert in seinem W-LAN-Telefon F1000 Drahtlos-Kommunikation mit Voice-Over-IP-Support – eine sinnvolle Kombination.

CeBIT HANNOVER 10.–16. 3. 2005

Nicht nur Computer-Firmen widmem sich dem Thema Wireless-LAN, auch Hersteller „brauner Ware“ (Hifi, Heimkino) und Automobilkonzerne haben die Vorzüge drahtloser Datenübertragung entdeckt. Unter dem Namen „Network on Wheels“ (NOW) entwickeln BMW, Audi, Daimler Chrysler, VW, Renault und Fiat einen Standard für die drahtlose Car-to-Car-Kommunikation auf Basis der 802.11-Funktechnologie. Heimkino-Fans können indes schon auf ein breites Angebot an W-LAN-Produkten, etwa drahtlose Media-Player zur Verbindung von PC und Hifi-Anlage, zurückgreifen. Philips und Samsung forschen bereits an Fernsehern mit W-LAN-Schnittstelle. Motorola und Oakley gehen noch einen Schritt weiter: Sie arbeiten gemeinsam an Sportkleidung mit Bluetooth-Schnittstelle.

Kodak Easyshare One

Erste Kompakt-Kamera funkt Fotos per W-LAN

ZUKUNFT JETZT: Ab Sommer steht Kodaks Easyshare One mit W-LAN-Modul in den Läden.

Was gestern noch Profis vorbehalten war, kommt im Sommer für rund 600 Dollar in den USA in den Handel: Kodak stellt mit der Easyshare One die erste Kompaktkamera mit W-LAN-Adapter (802.11b) vor. Für 99 Dollar Aufpreis kann man die SDIO-Karte in den SD-Kartenschlitz stecken und Fotos oder Videos vom 256 MByte großen internen Speicher an PC oder Drucker funken. Während die technischen Daten (4-Megapixel-Sensor, optisches 3-fach Zoom, 36 bis 108 mm) wenig spektakulär sind, glänzt die Easyshare One durch Innovationen: Das beliebig bewegliche 3-Zoll-Display ist zugleich Touchscreen. Ein spezieller Eingabestift bietet die Möglichkeit, E-Mails zu schreiben, Fotos anzuhängen und diese per W-LAN zu versenden. Als erste Kamera ist sie zudem mit Photoalben-Software ausgestattet. So hat man alle Erinnerungen ordentlich nach Alben oder Datum sortiert mit dabei.

Info: www.kodak.de, USA ab Sommer 2005, W-LAN-Modul 99 Dollar

Vorschau auf 802.11n

MIMO bekommt Geräte

Noch ist der Stadard 802.11n nicht endgültig definiert, da kämpfen bereits die Hersteller um die ersten Preview-Geräte mit der neuen MIMO-Technologie (Multiple Input, Multiple Output, siehe Beitrag auf 137). Belkin hat unter dem Label „Pre-N“ in Deutschland eine Desktop-Adapter-Karte (119 Euro), eine CardBus-Karte (99 Euro) sowie einen Router (159 Euro) vorgestellt. DLink zeigte erste Geräte in den USA: Der Router DI-624M und die CardBus-Karte WL-G650M. DLink bestätigte, dass erste Geräte in Deutschland im Sommer kommen.

NEUER STANDARD: DLinks Router DI-624M unterstützt MIMO.

Info: www.dlink.com, www.belkin.de

Breitband-Funknetze

Intel: Allianz für WiMAX

Der größte Halbleiterhersteller Intel und Chinas größter Hersteller von Telekommunikationsausrüstungen ZTE wollen das Breitbandnetzwerk WiMAX voranbringen. Auf Grundlage des „Rosedale“-Chips von Intel entwickelt ZTE Basisstationen und Infrastruktur für fest installierte Netzwerke (802.16-2004) und mobile Netze ((802.16e). ZTE beginnt nach eigenen Angaben noch in diesem Jahr mit dem Bau von Netzwerken in China, Osteuropa und Südostasien.

Info: www.intel.com, www.zte.com.cn/English/index.jsp

DSL-Router

Kabel, Funk & Powerline

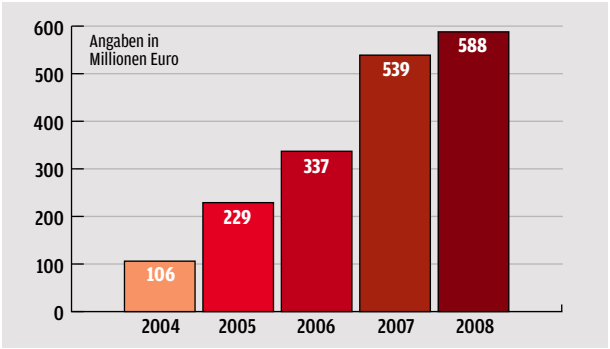
Er verbindet alles über viele Wege – verspricht Allnet für den All-In-One-DSL-Router namens ALL1681. Der Router soll sowohl via Ethernet, W-LAN (802.11b) oder ans Stromnetz angebundene PCs, Konsolen oder Hardware ins Internet bringen. Eine SPI-Firewall ist integriert. Er verfügt über vier 10/100Mbps-Ethernet-Anschlüsse, einen 54-Mbps-W-LAN-Access-Point sowie eine Powerline-Bridge für 230 Volt-Steckdosen, die 14 Mbps im Umkreis von 200 Metern ermöglichen soll.

ALL IN ONE: ALL1681 von Allnet verknüpft alles.

Info: www.allnet.de, verfügbar ab sofort, ca. 160 Euro

TREND

RFID treibt Umsätze nach oben



Quelle: Soreon Research

RFID IN DEUTSCHLAND: IT-DIENSTLEISTER ERWARTEN WACHSENDE UMSÄTZE VON DEN KLEINEN FUNKETIKETTEN. NEBEN DEN KOSTEN FÜR DIE HARDWARE WACHSEN DIE UMSÄTZE FÜR DIE BERATUNG.

ProSafe Access Point WG102

W-LAN-Referenz von Netgear: Superschnell & supersicher

Netzspezialist Netgear hat in den neuesten Access Point WG102 feinste Technik gepackt. Das Gerät ist offensichtlich speziell für die Bedürfnisse kleinerer Unternehmen ausgerichtet: Modernste Sicherheitsfunktionen machen Netzwerkverbindungen immun gegen mögliche Angriffe. So verfügt der WG102 neben VPN-Passthrough und MAC-Adressen-Filterung über Radius Server (802.1x) und Funktionen wie EAP TLS, TTLS und PEAP. Das Gerät ist bereits für WPA2-Verschlüsselung (802.11i) vorbereitet, die per Firmware-Update aktualisiert werden kann.

Der Access Point überträgt entsprechend dem Standard 802.11g mit 54 MBps. Mittels Super-G-Technologie können Daten mit Geschwindigkeiten von bis zu 108 MBps verschickt werden.

PROFI: Netgears WG 102 bietet viel für 120 Euro.

Der WG102 kann im Point-to-Point-Modus einen oder als-Point to-Mulitpoint-Bridge mehrere Access Points ansteuern. Dank Power over Ethernet (802.11af) kann er direkt über das Ethernetkabel mit Strom versorgt und dort abgestellt werden, wo die beste Reichweite erzielt wird. Die Antenne lässt sich zudem gegen reichweitenstärke Antennen auswechseln bzw. das Gerät als Repeater eingesetzt werden. Für das Management stehen die Protokolle SNMP MIB I und MIB II zur Verfügung sowie 802.11 MIB.

Info: www.netgear.de, verfügbar ab sofort, ca. 120 Euro

Digital oder analog?

Digitalsound im Kopfhörer

Toshiba und Motorola haben auf der CES-Show in Las Vegas das erste Modell für Bluetooth-Stereo-Kopfhörer vorgestellt, die derzeit noch nicht in Deutschland erhältlich sind.

USB UND LOS: Vivanco sendet auf 2,4 GHz.

Auf die Frequenz 2,4 GHz vertraut Zubehör-Hersteller Vivanco beim Set CHH 100. Per USB wird ein Digitalsender an die Audioquelle angeschlossen. Er sendet rund 30 Meter weit an den Kopfhörer. Die digitale Übertragung soll rauschfrei sein.

Info: www.vivanco.de, erhältlich ab sofort, ca. 60 Euro

Media-Adapter von Linksys

Erster HD-Video-Stream

Kostenpflichtigen Video-Streams den Weg ins Wohnzimmer bahnen will Linksys mit dem Breitband-Adapter New Wireless-G Media Link. Er unterstützt die neue Kopierschutztechnik DTCP-IP, die Intel erstmals vorgestellt hat. Der Adapter kann drahtlos Musik und Fotos übertragen, aber auch HD-Videos in MPEG4 und WMV wiedergeben.

Info: www.linksys.com, ab Sommer, Preis noch nicht bekannt

Funkbrücke von Conrad

Bluetooth get the Blues

Eine „Bluetooth-HiFi-Funkverbindung" bietet der Elektronikhändler Conrad an. Der akkubetriebene Bluetooth-Sender des taiwanesichen Herstellers Air2U wird per 3,5-mm-Klinkenstecker an mobile Geräte wie einen MP3-Player angeschlossen. Der Empfänger überträgt das Signal analog über einen Cinch-Stereo-Ausgang an die HiFi-Anlage.

Info: ww.conrad.de, sofort erhältlich, ca. 100 Euro

Kampf um den Stream

Audio-Receiver mit W-LAN

Bei 100 Euro wird sich der Preis wohl einpendeln, den man für einen Wireless Audio-Receiver wie den Noxon Audio von Terratec (siehe Interview unten) zahlen muss. Der Audio-Receiver verbindet den PC per W-LAN (802.11b) und die Hi-Fi-Anlage per Audio-Kabel. Hersteller wie SMC ziehen nach und bieten mit dem EZ-Stream MCWAA-B ebenfalls einen Audio-Receiver zum Konkurrenzpreis an. Auch dieser nutzt nur die WEP-Verschlüsselung.

EZ-STREAM: Verbindet PC und Stereo-Anlage.

Info: www.smc-europe.com/de/, erhältlich ab sofort, ca. 110 Euro

INTERVIEW

Wir benötigen einfache und kostengünstige Heimnetzwerke

„Alle portablen und mobilen Geräte werden W-LAN-fähig."

ULRICH GOBBERS, ENTWICKLUNGSCHEF TERRATEC ELECTRONIC GMBH

CHIP Sie haben gerade mit dem „NOXON Audio" ein Audio-Streaming-System für das Wohnzimmer vorgestellt. Wen stellen Sie sich dabei als Anwender vor?

Ulrich Gobbers Der NOXON Audio ist das ideale Produkt für jeden, der in seiner Wohnung über einen drahtlosen Zugriff auf das Internet und auf einen oder mehrere Rechner verfügt. Durch die Einfachheit der Installation und der Bedienung ist es auch ohne Fachwissen möglich, aus Wohnzimmer, Küche oder Schlafzimmer bequem auf Musikdaten auf der Festplatte seines Rechners und auf die Vielzahl der Internet Radiosender zuzugreifen.

CHIP Der Noxon erlaubt nur die wesentlich unsichere WEP-Verschlüsselung. Warum?

Ulrich Gobbers Zum Zeitpunkt der Entwicklung war WPA und erst recht WPA2 noch kein Thema. Wie Sie wissen, ist die Mehrzahl der Netzwerke im privaten Bereich unverschlüsselt oder höchstens WEP-verschlüsselt. Für die meisten Anwender stellt sich diese Frage also derzeit nicht.

CHIP Wann kann er auf WPA oder WPA2 umgerüstet werden?

Ulrich Gobbers Der NOXON Audio ist kostenoptimiert entwickelt worden. Nur deshalb kann er auch zu so einem günstigen Preis angeboten werden. Die Prozessor- und Speicherauslegung des NOXON Audio lässt ein Update auf WPA bzw. WPA2 nicht zu.

CHIP Andere Hersteller haben ihre Produkte nach dem WiFi-Multimedia WMM zertifiziert. Wann wird Terratec nachziehen?

Ulrich Gobbers Sobald die Notwendigkeit besteht, werden wir eine Zertifizierung durchführen.

CHIP Welches Problem muss als nächstes gelöst werden, damit sich Wireless im Wohnzimmer weiter durchsetzt?

Ulrich Gobbers Es müssen mehr kostengünstige Endgeräte angeboten werden. Außerdem muss das Thema Heimvernetzung – sei es drahtlos oder drahtgebunden – durch einfach umzusetzende Konzepte noch mehr in das Bewusstsein des Kunden gelangen.

CHIP Welche Produkte sind in drei Jahren W-LAN-Realität?

Ulrich Gobbers Alle portablen und alle mobilen Geräte werden über W-LAN-Fähigkeiten verfügen, dazu die meisten der stationären AV-Komponenten. Sie werden in der Lage sein, auf unkomplizierte Weise miteinander zu kommunizieren, um gemeinsam eine komfortable Schnittstelle zu allen verfügbaren digitalen Mediendaten darzustellen.

Info: Noxon Audio, ca. 110 Euro, http://entertainde.terratec.net

ITRIP UND BLUETRIP: **Ein kleiner Sender funkt vom iPod per Bluetooth an den Receiver Bluetrip.**

Zubehör

iPod überall: Jetzt funkt der Apple zur HiFi-Anlage

Frustriert haben deutsche iPod-Nutzer bislang auf das Angebot des US-Herstellers Griffin geblickt. Dessen schickes UKW-Modul iTrip für den iPod überträgt Musik auf einer freien FM-Frequenz – was in Deutschland verboten ist. Mit dem Bluetooth-Adapter BlueTrip schließt Griffin bald auch hierzulande die Funklücke: Die Empfangseinheit im Design des iTrip wird in den iPod gesteckt und sendet legal zehn Meter weit digital an den Empfänger. Über einen Stereo-Cinch-Ausgang oder einen optischen Ausgang lässt dieser die iPod-Liste dann über die HiFi-Anlage klingen.
Info: www.griffintechnology.com, noch nicht erhältlich, ca. 150 Euro

Click'n Share

Schnurloses Filesharing

Prototypen für kabelloses Peer-to-Peer-Filesharing hat der US-Hersteller Memsen vorgestellt. Die Flash-Speicher-Sticks mit dem Namen „Click'n Share" können auch ohne PC-Anschluss Daten auf Knopfdruck austauschen. Zum System gehören Monitore, auf denen Inhalte der Speicher angezeigt werden. Memsen sucht auf seiner Homepage Partner für eine neue Art der Werbung: Während ein Anbieter die Kundeninformationen ausliest, erhält der Stickbesitzer Unterhaltungsinhalte. Da der Hersteller keinerlei Angaben zur Art der schnurlosen Datenübertragung macht, ist die Absicherung des Systems noch äußerst fragwürdig.
Info: www.memsen.com

Günstiges von Genius

Drahtlose Design-Tastatur

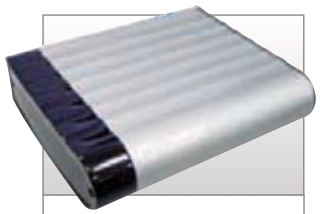
Von Genius stammt ein neues, drahtloses Tastatur-Maus-Set. Das Keyboard des „TwinTouch LuxeMate" besitzt acht Sondertasten und eine Wippe zur Steuerung von Multimedia-Playern. Ein Scrollrad ersetzt die Maus. Teil des Sets ist außerdem eine farblich angepasste Funkmaus. Ihr optischer Sensor bietet eine Auflösung von 800 dpi. Das symmetrische Gehäuse ist für Links- und Rechtshänder ausgelegt. Anschluss an den Windows-Computer gestattet ein USB-Empfänger, der Tastatureingaben und Mausklicks auf 27 MHz funkt.
Info: erhältlich ab sofort, www.genius-europe.com, ca. 50 Euro

KABELLOS: **Designtastatur und Maus von Genius.**

DVB-T-Empfänger

Digital-TV für unterwegs

Mit dem VideoMate DVB-U200 bringt der US-Hersteller Compro einen externen DVB-T-Empfänger auf den deutschen Markt. Die Installation und Stromversorgung erfolgt über USB 1.1 oder USB 2.0. Digitale terrestrische TV-Programme werden nach dem Anstecken der mitgelieferten Antenne über Autoscan automatisch ermittelt. Die installierte Software ermöglicht Videorecorder-Funktionen wie zeitgesteuerte Aufnahmen und zeitversetztes Betrachten der Sendungen (Timeshifting). Eine Fernbedienung gehört ebenso zum Lieferumfang wie alle Batterien, Kabel und ein umfangreiches Software-Paket.
Info: www.axanth.de, ab sofort verfügbar, ca. 100 Euro



TV TOTAL: **Compros DVB-T-Empfänger.**

T-DSL SpeedManager

Freeware findet W-LANs

Die Deutsche Telekom hat den Funktionsumfang der Gratis-Software T-DSL SpeedManager in der Version 5.2 um Optionen für die Nutzung von W-LANs erweitert. Das Programm soll alle am Standort eines Anwenders verfügbaren Funknetzwerke automatisch anzeigen und den Verbindungsstatus einblenden. Zudem will die Telekom die Einwahlprozedur in Wireless LANs vereinfacht haben.
Info: http://service.t-online.de/, Freeware

Für USB-Drucker

Günstiger Printserver

Der neue Wireless-G Print-Server von Linksys Netz bindet USB-Drucker ein. Geräte mit USB1.1. oder USB-2.0 lassen sich wahlweise über 10/100-Mbps-Ethernet oder W-LAN (802.11b oder g) ansteuern. Über einen Adhoc-Modus nimmt der Server auch Druckaufträge von kompatiblen Notebooks an. Die Daten können durch WEP-Verschlüsselung (64/128-Bit) oder auch durch Pre-Shared-Key-WPA geschützt übertragen werden. Ein Installations-Assistent hilft bei der Einrichtung.

AUCH OHNE PC: G Printserver von Linksys.

Info: www.linksys.de, erhältlich ab sofort, ca. 100 Euro

Download-Beschleuniger HSDPA

Schnellere UMTS-Karten

Der kanadische Mobilfunk-Spezialist Sierra Wireless bringt mit der Aircard 850 eine UMTS-Funkkarte für Notebooks auf den Markt, die den Download-Beschleuniger HSDPA (High Speed Downlink Packet Access) einsetzt. Statt maximal 385 KBps können damit bis zu drei MBps übertragen werden. Steht kein UMTS-Netz zur Verfügung, schaltet die Karte auf GPRS/GSM um. Eingebaut werden soll der HSDPA-Chipsatz MSM6275 von Qualcomm. Sierra kündigte die ersten Karten für Ende 2005 an. Nach ersten erfolgreichen Tests mit HSPA-Netzen in Atlanta, probiert derzeit Motorola das verbesserte Modulationsverfahren in Europa aus.

Info: www.sierrawireless.com, www.motorola.com

Mobiler Drucker

Fotos von Handy & PDA mit Bluetooth-Modul drucken

Canon investiert weiter in portable Tintenstrahldrucker: Der jetzt erhältliche Pixma IP90 wiegt nur 1,8 Kilogramm. Bei einer Auflösung von maximal 4.800 x 1.200 dpi druckt er bis zu zwölf Seiten pro Minute im Format DIN A4. Ein separat erhältlicher Bluetooth-Adapter (BU-10) ermöglicht die kabellose Übertragung vom PDA oder von Handys mit Direktdruckfunktion wie dem Nokia 6600.

MOBIL: Canons IP90 nimmt Fotos per Bluetooth an.

Info: www.canon.de, erhältlich ab sofort, ca. 250 Euro, Adapter ca. 80 Euro

TICKER-MELDUNGEN

BlackBerry: Jetzt auch für T-Mobiles MDA III

T-Mobiles Smartphone MDA III bietet jetzt auch BlackBerry-Unterstützung. Seit Anfang Februar können MDA-III-Besitzer ein entsprechendes Upgrade des Windows-Mobile-Betriebssystems downloaden. Damit lassen sich E-Mails, die im Firmen-Postfach eingehen, per Push-Verfahren an das Smartphone MDA III weiterleiten; der Anwender braucht also keine E-Mail-Abfrage mehr vorzunehmen. Weiterer Vorteil für T-Mobile-Kunden: Ebenfalls seit Anfang Februar umfasst der Monatsgrundpreis für den BlackBerry-E-Mail-Push-Service ein Datenvolumen von 5 statt 2 MByte, das für 2.500 E-Mails à 2 KByte ausreichen soll.

Info: www.t-mobile.de/business

MIMO-Antennen: Mehr Tempo mit RangeMax

Antennen, die sich dynamisch an die Netzwerkumgebungen anpassen, werden bald die W-LAN-Hardware deutlich beschleunigen. Dank der zu den Standards 802.11b und g kompatiblen RangeMax-Technologie sollen neben der Standard-Antenne sieben weitere intelligente MIMO-Antennen direkt auf dem Board 127 verschiedene Antennenmuster nachbilden können. Auf diese Weise lassen sich Aussetzer und Durchsatzeinbrüche aufgrund von Störungen, physikalischen Hindernissen oder Positionswechseln der Clients deutlich reduzieren. Mehr zu RangeMax lesen Sie auf 137.

Info: www.netgear.de

Multifunktion: Drucken per Bluetooth

Das Mulitifunktionsgerät Epson Stylus Photo RX620 wird auf Wunsch mit einem Bluetooth-Adapter ausrüstet, sodass sich mit dem Foto-Handy aufgenommene Schnappschüsse sofort ausdrucken lassen. Die Druckauflösung beträgt 5.760 x 1.440 dpi, bis zu 17 Seiten soll der RX620 pro Minute bedrucken. Das Gerät, das außerdem als Scanner und Kopierer fungiert, ist zur Bildkontrolle mit einem 2,4-Zoll-Display ausgestattet und kostet rund 300 Euro.

Info: www.epson.de/product/allinone/

Neue Chipsätze: Intel setzt auf W-LAN

Im zweiten Quartal 2005 will Intel die neuen Chipsätze 945 (Codename „Lakeport“) und 955 (Codename „Glenwood“) mit W-LAN-Komponenten vorstellen. Die Nachfolger der aktuellen Chipsätze 915 und 925 sollen Kern des „East-Fork“-Produktkonzepts werden, das Intel gerade für den Desktop-Bereich entwickelt und ähnlich wie die Notebook-Lösung Centrino vermarkten will. In die East-Fork-Produkte soll auch ein Dreiband-Chipsatz für alle gängigen W-LAN-Typen 802.11a,b und g integriert werden.

Info: www.intel.com, www.theinquirer.net

Smart Antennas: Weiter und schneller funken

Mit Hilfe des Chipsatzes AR5005VL des kalifornischen Herstellers Atheros Communicatios und der MIMO-Technik, mit der bis zu vier Smart Antennas arbeiten, sollen Datenraten von bis zu 50 MBit/s netto erreicht werden. Verfügt die Gegenseite nicht über MIMO-fähige Hardware, sind laut Atheros immer noch 27 MBit/s Datendurchsatz drin. Der Preis des Chipsatzes in der 10.000er Unit liegt bei etwa 20 Dollar.

Info: /www.atheros.com/news/AR5005VL.html

Roaming-Abkommen

630 Hotspots vereint

Das erste große W-LAN-Roaming-Abkommen haben O2 und Vodafone abgeschlossen. Demnach können die Kunden gemeinsam die rund 630 Hotspots der Mobilfunkanbieter nutzen und jeweils bequem über die Handyrechnung bezahlen. Roaming-Gebühren fallen dabei nicht zusätzlich an. Neben Hotels großer Ketten wie Best Western (im Foto: Jena) umfasst das Abkommen auch Lufthansa-Lounges.

Info: www.vodafone.de, www.o2online.de/goto/wlan

HOT(EL)SPOT: Bezahlt wird via Handyrechnung.

Smartphone Treo 600

W-LAN und GPRS zugleich

Gleichzeitigen Betrieb von W-LAN und GPRS/GSM ermöglicht eine Erweiterung für Palmones Smartphone Treo 600 des texanisches Zubehörherstellers Enfora: Der aufsteckbare W-LAN-Adapter „WiFi-Sled" bezieht aus einem Akku Energie für bis zu drei Stunden Vollbetrieb. Das 150 Dollar teure Gerät ist derzeit nur in den USA für den Treo 600 erhältlich.

Info: www.enfora.com, Start in Deutschland noch nicht bekannt

Network on Wheels

Funknetz im Automobil

Ein erster Standard für Funkverbindungen ins Auto ist dem Bundesministerium für Bildung und Forschung vier Millionen Euro wert. Die Universität Mannheim, die TU Karlsruhe sowie Siemens, NEC und Fraunhofer Institut entwickeln ihn im Projekt „Network on wheels" auf Grundlage der 802.11-Funktechnologie und des Internetprotokolls IPv6.

Info: www.car-to-car.org, www.dlr.de

Kleiner Alleskönner

W-LAN für unterwegs

Drei Betriebsmodi bietet der neue Wireless Travel Access Point ALL0274 von Allnet. Er kann als reiner W-LAN-Client etwa das Notebook unterwegs mit dem Funknetz verbinden.

REISE-RIESE: Der ALL027 von Allnet.

Über einen Schalter wird das nach IEE802.11g-Standard arbeitende Gerät zum Acess Point oder zur Kombination aus Access Point und Router mit 54 MBit/sek. Entgegen anders lautender Meldungen verschlüsselt das Gerät tatsächlich nach WEP (64/128 Bit).

Info: www.allnet.de, ca. 50 Euro, sofort erhältlich

INTERVIEW

Bei O2 sind Kunden wesentlich zufriedener als bei T-Mobile

O2 hat gerade mit 32 Prozent mehr neuen Kunden ein Rekordquartal erlebt. Offensichtlich macht der Anbieter seine Kunden auch am glücklichsten. Das ergab eine soeben veröffentlichte repräsentative Studie des Marktforschungsinstituts dpm-team. Während nur 13 Prozent der O2-Kunden wechseln wollen, würden 29 Prozent gerne E-Plus verlassen. Besonders deutlich wird der Abstand bei der Kundenzufriedenheit: 84 Prozent der O2-Kunden sind sehr zufrieden oder zufrieden. Bei T-Mobile geben dies nur 64 Prozent an.

„Zufriedenheit ist eine Voraussetzung für nachhaltigen Erfolg"

KATHRIN POSNANSKI
MARKTFORSCHERIN DPM-TEAM

CHIP Wann sind Kunden zufrieden mit ihrem Anbieter?

Kathrin Posnanski Zufriedenheit ist ein sehr subjektives Gefühl. Vereinfacht ergibt sich Kundenzufriedenheit aus der Differenz von persönlichen Erwartungen und Vorstellungen vor dem Kauf und der subjektiv wahrgenommenen Differenz nach dem Kauf. Die Höhe der Abweichung zwischen Erwartung und Leistung bestimmt den Grad der Zufriedenheit bzw. der Unzufriedenheit. Aus der Perspektive der Anbieter ist Kundenzufriedenheit eine Voraussetzung für nachhaltigen Erfolg am Markt. Denn Neukunden zu gewinnen ist in der Regel teuerer als Bestandskunden zu halten.

CHIP Ihre Studie belegt, dass die Kunden von O2 mit deutlichem Abstand am zufriedensten sind. Warum?

Kathrin Posnanski O2 schafft es optimal auf seine Zielgruppe, die im Vergleich zu den anderen Anbietern sehr jung ist, einzugehen und deren Wünsche und Bedürfnisse bestmöglich zu erfüllen.

CHIP Was macht der Marktführer T-Mobile falsch, wenn er am schlechtesten abschneidet? Muss T-Mobile jetzt fürchten, dass viele Kunden ihren Tarif wechseln?

Kathrin Posnanski Kunden von T-Mobile sind im Schnitt etwas älter und haben besondere Erwartungen, die erfüllt werden müssen: Qualifizierte Beratung und Erreichbarkeit von persönlichen Ansprechpartnern vor Ort sind wichtig. Wird auf diese Kundenwünsche eingegangen, kann T-Mobile auch zukünftig seine Marktposition sichern, da das hohe Ansehen der eigenen Kunden ein solides Polster darstellt.

CHIP Wie haben denn die Netzbetreiber auf die Ergebnisse Ihrer Studie reagiert?

Kathrin Posnanski Alle hat der große Vorsprung von O2 überrascht. Die vier großen Anbieter haben mit hohem Interesse schnell mit uns Kontakt aufgenommen. Sämtliche Anbieter haben daraufhin die kompletten Studienergebnisse von uns erhalten.

Mitmachen & gewinnen!

Ihre Meinung ist uns wichtig: Wie hat Ihnen diese Zeitschrift aus der Reihe „CHIP Professionell“ gefallen? Helfen Sie uns dabei, das Heft noch besser zu machen. Gehen Sie einfach auf **www.chip.de/wirelessumfrage** und füllen Sie den digitalen Fragebogen aus. Mit etwas Glück gewinnen Sie einen der attraktiven Preise.

Preise im Gesamtwert von 1.900 Euro gewinnen!

1x ISDN-Netzwerkkamera von Mobotix

Die M10-Web kann über ISDN, GSM, DSL, W-LAN oder Ethernet ganz problemlos ins Netzwerk integriert werden. Durch den Megapixel-Sensor mit 1280 x 960 Bildpunkte liefert die M10-Web Bilder in sehr guter Farbqualität. Die freie Wahl der Belichtungs-messzonen erlaubt die automatische Anpassung an schwierige Gegenlichtverhältnisse.

Wert: 930 Euro

10x Software von Panda

5x Panda Antivirus Titanium 2005: Schützt Ihren PC vor allen Viren, Würmern und Trojanern.
5x Panda Internet Security 2005: Bietet Rund-um-Schutz für PCs und serverlose Netzwerke. Zur Software gehören eine Firewall, ein Spyware-Blocker und ein Anti-Spam-Modul. Ein Web-Content Filter und Anti-Dialer-Funktionen runden das Paket ab.

Gesamtwert: 600 Euro

1x Wireless Kit von D-Link

Mit dem DWL-926 werden Sie mobil. Es enthält den 108 Mbit Wireless DSL Internet Gateway DI-624 plus Switch sowie die 108 Mbit Wireless CardBus Card DWL-G650. Damit haben Sie alles, um über Ihre DSL-Verbindung ein Wireless LAN aufzubauen.

Wert: 120 Euro

10x Bücher von Franzis

5x „WLANs optimal einsetzen“: Sie erfahren alles über drahtlose Netzwerke.
5x „Linux im Windows-Netzwerk“: liefert praktisches Know-how für Umstieg auf und Einstieg in Linux im Netzwerkbereich.

Gesamtwert: 260 Euro

UND SO GEHT'S:

1. Online gehen: Rufen Sie unsere Umfrage im Internet unter der folgenden Adresse auf:

www.chip.de/wirelessumfrage

2. Fragebogen ausfüllen: Füllen Sie den Fragebogen aus und geben Sie Ihre Daten und E-Mail-Adresse an, damit wir Sie im Falle eines Gewinns benachrichtigen können.

3. Gewinnchance: Wer den Fragbogen vollständig ausfüllt, nimmt automatisch an der Verlosung teil.

Teilnahmeschluss: 17. April 2005

Mitarbeiter der Vogel Burda Communications und der beteiligten Sponsoren dürfen nicht teilnehmen. Eine Barauszahlung der Gewinne ist nicht möglich. Der Rechtsweg ist ausgeschlossen.

KNOW-HOW | INHALT

Drahtlose Zukunft 14
Schluss mit dem Kabelsalat in Arbeitszimmer und Wohnung. Lesen Sie hier alles über Funknetze.

TCP/IP konfigurieren 20
Damit Ihre Geräte drahtlos funken, müssen Sie IP-Adressen vergeben. Wie, das erfahren Sie hier.

Mit Minis ins Web funken 22
Sie wollen auch unterwegs auf Kabel verzichten? Kein Problem, wenn Sie diese Seiten lesen.

Alles über Wireless Fidelity 26
Hotspots gehört die Zukunft. Wie Sie diese Technik richtig und sicher nutzen, steht in diesem Beitrag.

Nah dran mit Bluetooth 28
Mit dieser Funktechnik können Sie Ihr W-LAN ausreizen. Hintergründe, Tipps & Tricks stehen hier.

Blackberry für Jedermann 32
Bislang profitierten nur Firmen von Blackberry. Jetzt steht die Technik allen zur Verfügung.

WiMAX – das Super-W-LAN 40
So sieht die Zukunft drahtloser Netzwerke aus – und so profitieren Sie davon.

Keine Angst vor Chips 42
RFID ist ein Reizwort für Datenschützer. Richtig genutzt bieten die funkenden Chips nur Vorteile.

CHIP AUTOR → Peter_Klau@t-online.de

Peter Klau ist Programmierer und Netzwerkverwalter. Er arbeitet seit etwa 15 Jahren als freiberuflicher IT-Journalist und Buchautor. Mittlerweise sind von ihm weit mehr als 30 Bücher aus den Bereichen Computer, Internet, Lifestyle, Hobbys und Reisen erschienen sowie zahlreiche Artikel in Fachzeitschriften. Peter Klau arbeitet zudem als Dozent an der VHS-Dortmund.

CHIP → DVD-CODE W-LAN

- → **W-LANs finden** Mit dem kostenlosen Tool Network Stumbler spüren Sie drahtlose Zugangspunkte (Hotspots) in Ihrer näheren Umgebung auf.
- → **Linux für W-LANs** Die Auditor Security Suite ist eine Linux-Live-Distribution für Admins. Alle wichtigen Tools, wie Sniffer und Analyzer sind integriert.
- → **WEP-Schlüssel checken** Mit AirSnort testen Sie Ihre WEP-Verschlüsselung. Das Tool fängt Netzwerk-Verkehr ab und berechnet daraus gültige WEP-Keys.

Kabel war gestern, die Zukunft ist mobil und drahtlos. Funknetze erleben deshalb ein rapides Wachstum. Lesen Sie, welche Technik dahintersteckt und nach welchen Prinzipien drahtlose Netzwerke funktionieren.

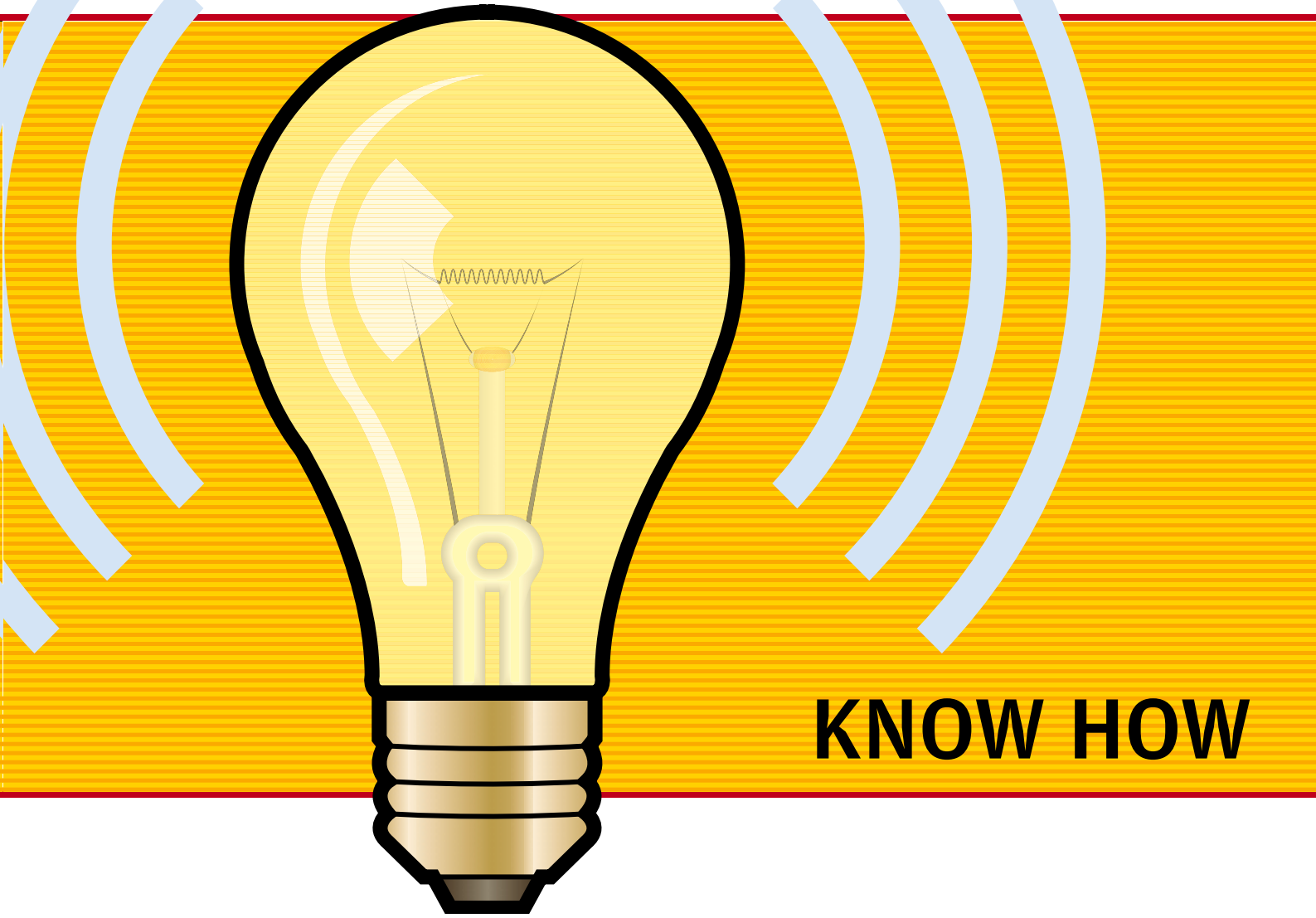
Drahtlose Netzwerke

Wireless – die

Drahtlose Netzwerke funktionieren nach dem gleichen Prinzip wie schnurlose Telefone. Ein Transceiver (die Kombination aus Transmitter und Receiver) sendet auf einer bestimmten Frequenz elektromagnetische Wellen, die über Antenne sowohl abgestrahlt als auch empfangen werden. Auch Radios und Fernseher arbeiten in ähnlicher Weise – mit dem einzigen Unterschied, dass die Senderichtung in diesem Fall eine Art „Einbahnstraße“ ist.

Datenfunk – Signale durch die Wand

Daten werden heute in Computer-Netzwerken noch hauptsächlich mit Hilfe von Kupferkabeln übertragen. Doch in vielen Fällen ist es sinnvoll, die Kabel durch elektromagnetische Wellen zu ersetzen. Drahtlose Netzwerke eignen sich besonders gut für Einsatzorte, die per Kabel nur schwer zu erreichen sind. Die normale Reichweite einer drahtlosen Verbindung beträgt bis zu 300 Meter im freien Gelände und bis zu 100 Meter in Gebäuden. Mit Verstärkern und besonderen Antennen lässt sich die Reichweite jedoch beträchtlich vergrößern.



KNOW HOW

Zukunft ist drahtlos

Technisch gesehen gibt es zur Einrichtung eines drahtlosen Netzwerks einige Alternativen. Systeme wie HomeRF, HiperLAN, DECT oder Bluetooth kämpfen um die Gunst der Käufer. Bis auf DECT für schnurlose Telefone und Bluetooth für kleinere Netzwerke werden für ein Wireless LAN jedoch hauptsächlich Netzwerke nach dem IEEE-Standard 802.11 verwendet. Im Vergleich zu normalen Radio- und Fernsehsignalen gibt es im W-LAN jedoch einige Unterschiede:

Statt Audio- oder Videosignalen werden in einem Wireless LAN Daten übertragen.

Aus Sicherheitsgründen werden die W-LAN-Signale gespreizt. Dadurch wird ein weitaus größerer Frequenzbereich genutzt, als zur eigentlichen Übertragung notwendig ist.

Drahtlose Netzwerke benutzen andere Frequenzen als Radio- oder Fernseh-Geräte.

Frequenzen für die drahtlose Übertragung

Sollen die Daten mit Hilfe elektromagnetischer Wellen übertragen werden, lässt sich das auf vielen Frequenzen erreichen. Dabei besitzt jeder Frequenzbereich seine ganz spezifischen Vor- und Nachteile.

Die Funkübertragung beginnt mit wenigen KHz, dem so genannten Very-Low-Frequency-Bereich (VLF). Diese Frequenzen können sich, ebenso wie die des Langwellen-Bereichs (Low Frequency, LF) entlang der Erdkrümmung und im Wasser ausbreiten. Letzteres ist auch der Grund, warum diese Frequenzen zur Kommunikation etwa bei U-Booten eingesetzt werden.

Höhere Frequenzen – in den Bereichen zwischen 174 und 230 MHz (Very High Frequency, VHF) und zwischen 470 und 790 MHz (Ultra High Frequency, UHF) – werden für die Übertragung analoger TV-Signale benutzt. Auch der digitale Rundfunk (Digital Audio Broadcast, DAB) und das digitale Fernsehen (Digital Video Broadcast, DVB) nutzen diesen Frequenzbereich. GSM-Mobiltelefone arbeiten mit 1.800 MHz.

Der Super High Frequency-Bereich (SHF) liegt zwischen 2 und 40 GHz. Dieser Bereich wird für Mikrowellen-Verbindungen verwendet, typische Anwendungen sind Satelliten-Verbindungen. Einige Systeme arbeiten bereits im Extremely →

High Frequency-Bereich (EHF), der schon sehr nahe am Infrarot-Bereich liegt. Das Frequenzband reicht von 30 bis 275 GHz.

Im Infrarot-Bereich (IF) werden neben der leitungsgebundenen Übertragung mit Glasfasern auch drahtlose Verfahren eingesetzt, zum Beispiel bei der Datenübertragung zwischen Gebäuden mit Hilfe von Lasern. Die am weitesten verbreitete Infrarot-Technologie IrDA (Infrared Data Association) arbeitet mit einer Wellenlänge von 800 bis 900 nm. Damit werden Geräte wie Notebooks, PDAs und Handys direkt miteinander vernetzt.

Der große Nachteil der Infrarot-Technik besteht jedoch darin, dass zwischen den Geräten eine Sichtverbindung (Line Of Sight, LOS) bestehen muss und die Geräte außerdem sehr nahe beieinander positioniert sein müssen. Moderne drahtlose Netzwerke lösen dieses Problem, indem sie Frequenzen benutzen, die weit oberhalb des sichtbaren Bereichs liegen. Dadurch wird die Wellenlänge so klein, dass die Signale mühelos auch feste Objekte wie zum Beispiel Wände durchdringen.

Zum Vergleich: Zur Übertragung von Daten werden in drahtgebundenen Netzwerken verdrillte Kupferadern mit Frequenzen von 100 MHz benutzt. Koaxialbabel, etwa beim Kabelfernsehen, übertragen mit mehreren hundert MHz. Noch schneller geht es bei Glasfaserleitungen, die die Daten mit mehreren hundert Terahertz (THz) übertragen.

Funkfrequenzen sind zentral organisiert

Die meisten Funkfrequenzen sind heute belegt, deshalb sind nutzbare Frequenzen ein kostbares Gut. Obwohl nationale Interessen einer einheitlichen Regelung häufig im Wege stehen, ist die International Telecommunications Union (ITU) in Genf für die weltweite Vergabe der Frequenzen zuständig. Zur besseren Koordinierung wurde die Welt von der ITU in drei Regionen aufgeteilt:

Region 1: Europa, Naher Osten und die Staaten der früheren Sowjetunion

Region 2: Nordamerika, Südamerika und Grönland

Region 3: Asien, Australien und Neuseeland

Innerhalb der Regionen sind wiederum regionale Institutionen für die Regelung zuständig. In Europa ist das die CEPT (European Conference for Posts and Telecommunications Administrations). In der regelmäßig von der ITU abgehaltenen World Radio Conference (WRC) werden die Frequenzbelegungen für die drei Regionen festgelegt und weltweite Standards vorbereitet. Da in den einzelnen Regionen die Frequenzen nicht harmonisieren, werden für bestimmte Techniken oft andere Frequenzbereiche genutzt. Eine Übersicht zeigt die Tabelle auf 17.

Die Kanäle für Wireless LAN

802.11-kompatible W-LANs benutzen zur Datenübertragung die Frequenzen des ISM-Bands, das in 13 Kanäle aufgeteilt ist (siehe Tabelle oben). ISM steht für „Industrial, Scientific, Medical"; dieser Frequenzbereich wird somit auch in der Industrie, Wirtschaft und Medizin verwendet. Von den international zugewiesenen ISM-Frequenzen werden die Frequenzbereiche 2.400 bis 2.500 MHz und 5.150 bis 5.725 MHz für W-LAN-Anwendungen genutzt. Der interessanteste Bereich um 2,4 GHz steht fast weltweit für W-LANs zur Verfügung, auch wenn zahlreiche nationale Restriktionen in punkto Sendeleistung und Bandbreite existieren.

Allerdings senden auch elektrische Garagentore, Mikrowellenherde und Kurzwellenstrahler für medizinische Zwecke in diesem Frequenzbereich. Durch die dabei unvermeidlichen Störstrahlen kann es bei W-LAN-Hardware in der Nähe von Hochfrequenzgeräten zu Störungen bei der Datenübertragung kommen.

KNOW-HOW

Die ISM-Kanäle

Kanal	Frequenz
1	2.412 MHz
2	2.417 MHz
3	2.422 MHz
4	2.427 MHz
5	2.432 MHz
6	2.437 MHz
7	2.442 MHz
8	2.447 MHz
9	2.452 MHz
10	2.457 MHz
11	2.462 MHz
12	2.467 MHz
13	2.472 MHz

Wie Sie aus der Tabelle ablesen können, beträgt der Abstand zwischen den einzelnen Kanälen gerade mal 5 MHz. Sollen in einem engeren Umfeld mehrere W-LAN-Netzwerke betrieben werden, empfiehlt es sich, zur Vermeidung von Interferenzen einen Abstand von sechs Kanälen einzuhalten. Im Gegensatz zu den 13 ISM-Kanäle in Deutschland sind andere Länder viel restriktiver: In Frankreich sind nur die Kanäle 10 bis 13, in den USA die Kanäle 10 und 11 freigegeben.

Senden und empfangen ohne Wellensalat

Die in den Funknetzen gesendeten Signale haben die Eigenschaft, sich gleichmäßig auszubreiten und zu überlappen. Besonders in stark genutzten Netzwerken, wie man sie in Büros oder Coffee-Shops antrifft, senden häufig einige Dutzend Stationen ihre Signale auf der gleichen Frequenz.

Abhilfe schafft die Bandspreizung: Das Spread-Spectrum-Übertragungsverfahren wurde einmal für militärische Anwendungen entwickelt, um Daten möglichst abhörsicher zu übermitteln. Durch das Aufspreizen der Daten über einen sehr viel größeren Frequenzbereich als den des Nutzsignals benötigt man eine geringere Sendeleistung. Mit dieser Technik wird aber nicht nur das Orten und Abhören des Senders erschwert, sondern auch der Einfluss von schmal- und breitbandigen Störquellen minimiert. Für die Übertragung von Daten in einem Wireless LAN haben sich drei – allerdings nicht kompatible – Varianten der Spread-Spectrum-Technik durchgesetzt:

Frequency Hopping Spread Spectrum (FHSS)

Direct Sequence Spread Spectrum (DSSS)

Orthogonal Frequency Division Multiplexing (OFDM)

Die ersten IEEE-802.11-WLANs setzten dazu – ebenso wie Bluetooth – auf FHSS. Das Frequenzsprungverfahren ist ein äußerst robustes und fehlertolerantes Verfahren. Dabei werden die Datenpakete zwischen den Kommunikationspartnern auf ständig wechselnden Trägerfrequenzen übermittelt. Dadurch kann auf Störungen durch Geräte, die ihre Signale im selben Frequenzspektrum übermitteln, reagiert werden. Nach einem erfolglosen Sendeversuch eines Datenpaketes kann dieses also auf einer anderen Trägerfrequenz erneut übertragen werden. Durch

FHSS ließen sich Übertragungsraten von bis zu 2 MBit/s erzielen. Dieses Verfahren ist jedoch inzwischen veraltet, Komponenten mit dieser Übertragungstechnologie werden kaum noch angeboten.

Die nach wie vor wichtigen IEEE-802.11b-Produkte setzen durchweg auf DSSS als Übertragungstechnologie. Diese Technik unterbindet das Abhören und zeichnet sich durch eine erheblich reduzierte Anfälligkeit gegenüber Störsignalen aus. Das liegt an der Spreizung des zu übertragenden Signals über mehrere Frequenzbereiche. Bei dem DSSS-Verfahren wird das 2,4-GHz-Frequenzband in 22 bis 26 MHz breite Frequenzbänder unterteilt. Mit DSSS lassen sich unter Einsatz ausgefeilter Modulationsverfahren Bruttodatenraten von 11 MBit/s erzielen. Aus Gründen der Abwärtskompatibilität (und beim Verbindungsaufbau) müssen IEEE-802.11b-Geräte jedoch noch die Datenraten bis herab zu 1 MBit/s beherrschen.

OFDM ist ein Modulations-Verfahren zur drahtlosen Funkübertragung großer digitaler Datenmengen. Bei dieser Technik wird das Signal in viele kleine, eng beieinander liegende Einzelsignale (Unterträger) aufgeteilt, die parallel über verschiedene Frequenzen übertragen werden. OFDM verringert das so genannte Übersprechen (crosstalk) bei der Signalübertragung. Zum Einsatz kommt OFDM in den IEEE-802.11a-W-LANs im 5-GHz-Band. Seit Mai 2001 darf OFDM nach einer Lockerung der FCC-Vorschriften auch im 2,4-GHz-Band genutzt werden, steht damit also auch den 802.11b- und -g-Netzen offen.

So breiten sich die Funksignale aus

In leitungsgebundenen Netzwerken breiten sich die Signale entlang eines Leiters (Kabel, Glasfaser etc.) aus. Deshalb lassen sich bei einem Kabelnetzwerk auch sehr präzise Vorhersagen über die Stärke und Reichweite eines Signals machen. Bei drahtlosen Netzwerken ist die Ausbreitung des Signals von vielen Faktoren abhängig, etwa Gebäuden, Bäumen, Gelände und atmosphärische Bedingungen. So lange sie nicht daran gehindert werden, breiten sich Radiowellen gleichmäßig nach allen Seiten (isotrop) aus. Neben der Dämpfung (Leistungsverlust bei zunehmendem Abstand vom Sender) treten bei der drahtlosen Signalausbreitung noch die folgenden Effekte auf:

Abschattung (Shadowing): Ein großes Objekt im Sendebereich verhindert die freie Signalausbreitung. Bei hoher Frequenz können selbst kleine Objekte eine Abschattung bewirken.

Reflektion (Reflection): Ist ein Objekt im Verhältnis zur Wellenlänge groß genug, wird ein Signal reflektiert beziehungsweise ein kleiner Teil absorbiert. Vorteil: In Städten kann die Reflektion den Empfang in einigen Gebieten erst ermöglichen.

Streuung (Scattering): Bei diesem Effekt wird das Signal an einem Objekt in mehrere schwächere Signale aufgespalten, die in verschiedene Richtungen laufen.

Beugung (Diffraction): Die Funksignale werden an den Kanten von Objekten von ihrer ursprünglichen Ausbreitungsrichtung abgelenkt.

So funktioniert die Bluetooth-Technik

Bluetooth ist ein Netzwerk-Standard für den Nahbereich, der auf der gleichen 2,4-GHz-Frequenz sendet wie Geräte nach dem Standard IEEE 802.11b und 802.11g. Die Technik ist gut geeignet zum Download von Bildern von einem digitalen Fotoapparat, zum Synchronisieren von Daten zwischen Desktop-PC und Handheld-Computern oder zum einfachen Datenaustausch zwischen Desktop-PCs, die nicht durch ein LAN oder Wireless LAN verbunden sind (lesen Sie mehr ab 28).

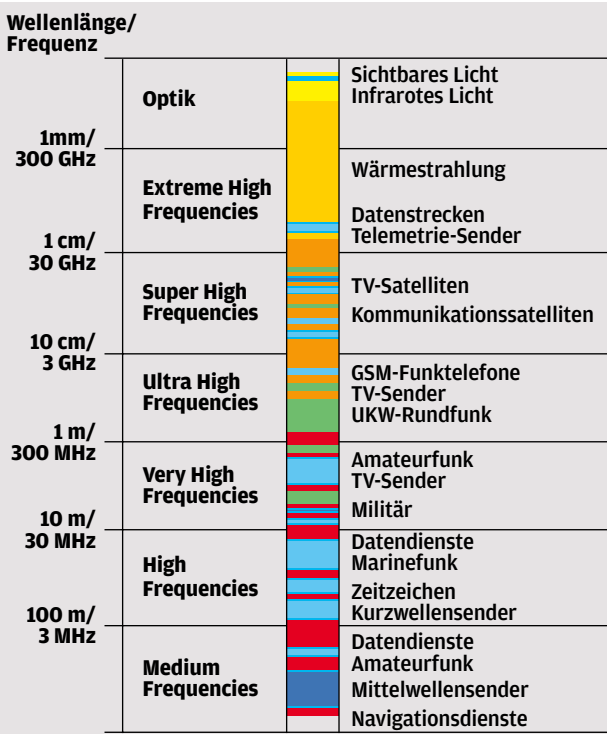
Die Datenübertragungsrate beträgt theoretisch 1 MBit/s. Moderne Bluetooth-Adapter für den USB-Port lassen ihre erst vor wenigen Jahren eingeführten Vorgänger in punkto Reichweite deutlich hinter sich. Die Besten unter ihnen überbrücken als Klasse-1-Funker mit nur 100 Milliwatt effektiver →

KNOW-HOW

Frequenzbelegungen der CEPT

	Frequenzen in Europa
Mobiltelefone	GSM 890 bis 915 MHz 935 bis 960 MHz 1.710 bis 1.785 MHz 1.805 bis 1.880 MHz
Schnurlose Telefone	CT2 864 bis 868 MHz DECT 1.880 bis 1.900 MHz
Wireless LAN	IEEE 802.11 2.400 bis 2.483 MHz Hiperlan 1 5.150 bis 5.350 MHz 5.470 bis 5.725 MHz

Wer auf welcher Frequenz funkt



GUT SORTIERT: Öffentliche und nicht öffentliche Betreiber teilen sich das verfügbare Frequenzspektrum auf.

Illustration: CHIP S. Schönberger

Sendeleistung mühelos 200 Meter, obwohl die Technik ursprünglich nur für 100 Meter ausgelegt wurde.

Bluetooth benutzt ebenso wie die ersten IEEE-802.11-Wireless-LANs das Frequenz-Hopping; es wechselt also 1.600mal in der Sekunde die Frequenz. Das macht das System relativ unanfällig für Interferenzen und andere Störungen – und zwar auch wenn einige Bluetooth-Transceiver in einem engen räumlichen Areal gemeinsam funken.

Die Bezeichnung „Bluetooth" ist ein Markenname und kein IEEE-Standard. Allerdings wurde von der Wireless Personal Area Network (WPAN) Working Group 2002 der Standard IEEE 802.15.5 abgesegnet, der eine Teilmenge der von der Bluetooth Special Interest Group (SIG) entworfenen Technik ist. Als Konkurrent beziehungsweise Nachfolger wird ZigBee gehandelt, eine Nahfunk-Technik, die aufgrund ihrer stromsparenden Eigenschaften gegenüber Bluetooth im Vorteil ist (mehr zu ZigBee lesen Sie im Artikel ab 118).

Die wichtigsten Mobilfunknetze in Deutschland

Neben den IEEE-Funknetzen existieren noch weitere Funknetzwerke in Deutschland und Europa. GSM und UMTS sind die wichtigsten öffentlichen Mobilfunknetze zur Übertragung von Sprache und Daten. „Öffentlich" bedeutet, dass jeder diese Netze benutzen darf – im Gegensatz zu den nicht öffentlichen Netzen wie Seefunk, Flugfunk und Satellitenfunk. Das Mobilfunknetz GSM gibt es in Deutschland seit 1992, es ist Nachfolger des im Jahre 2000 abgeschalteten C-Netzes.

KNOW-HOW

W-LAN versus Bluetooth

IEEE 802.11 und Bluetooth – das sind zwei Funktechnologien, die unterschiedliche Ziele verfolgen und deshalb auch in Zukunft nebeneinander existieren werden. Während es bei Bluetooth um die Kommunikation zwischen ganz unterschiedlichen elektronischen Geräten über eine relativ kurze Distanz geht, handelt es sich bei IEEE 802.11 um eine Netzwerktechnologie, die direkt auf dem bestehenden Ethernet aufsetzt.
Die beiden Technologien im Überblick:

IEEE 802.11	Bluetooth
Hohe Datentransferrate von 54 Mbps	Datentransferrate von bis zu 1 Mbps
Reichweite von 30-100 m im Indoor-Bereich (je nach Bausubstanz). Im Outdoor-Bereich Radius bis zu 300 m.	Reichweite mit optimaler Datentransferrate typischerweise von 100 m.
Größere und komplexere Sende- und Empfangseinheiten.	Miniaturisierte, Strom sparende Sende- und Empfangseinheiten.

GSM-Telefone benutzen den Frequenzbereich um 900 MHz (D1, D2) oder 1.800 MHz (E plus, E2) mit einem Kanalabstand von 200 kHz, um Sprache und Daten digital in GMSK-Modulation (Gaussian Minimum Shift Keying) mit der nächsten

KNOW-HOW

Zukunftsmusik – neue Technik für Funknetzwerke

Diese Funktechnologien könnten die Zukunft prägen:
802.11n Die Evolution der Standards 802.11a und 802.11g soll die Datenübertragungsrate auf zunächst 108 und später 320 MBit/s hochtreiben. 2005 sind erste Ergebnisse zu erwarten, der Standard wird wohl erst Ende 2006 verabschiedet.
WiMAX – das Stadtnetz WiMAX ist eine Weiterentwicklung der Funk-LANs, basiert auf der A-Version des Standards 802.16 und zeichnet sich durch eine Übertragungsgeschwindigkeit von bis zu 74 MBit/s aus – bei einer Reichweite von bis zu 50 Kilometer. Der Standard 802.16 weist Übertragungsfrequenzen zwischen 10 und 66 GHz aus, die A-Version definiert Frequenzen zwischen 2 und 11 GHz und die B-Version zwischen 5 und 6 GHz. Damit wäre WiMAX bis zu 50mal schneller als DSL, 200mal schneller als UMTS und 1.300mal so schnell wie GPRS (mehr zu WiMAX lesen Sie ab 40).

Das WiMAX-Forum, das sich um die Standardisierung von WiMAX bemüht, will die Entwicklung für alle 802.16-Versionen vorantreiben. Ihm gehören mehr als 100 Mitglieder an, darunter Intel, Nokia und Siemens Mobile.

International laufen WiMAX-Projekte auf Hochtouren. In Deutschland gibt es zwar bisher keine konkreten Pläne, Lizenzen mit Frequenzen für WiMAX anzubieten, weltweit aber scheint sich schon 2005 ein Siegeszug von WiMAX abzuzeichnen. Mit seinen Reichweiten und Übertragungsbandbreiten wird WiMAX nicht nur die Grenzen der 802.11-W-LAN-Standards überwinden, sondern auch zu einer Verschmelzung von Mobilfunk und Festnetz beitragen.
HSDPA – der Turbo für UMTS UMTS ist in Europa noch gar nicht richtig in Schwung gekommen, da steht schon der Nachfolger „High Speed Downlink Packet Access" (HSDPA) vor der Tür. Die von Nokia entwickelte Technik soll vor allem dem Handy-Fernsehen den Durchbruch bringen. Wenn HSDPA etwa Mitte 2005 einsatzbereit ist, werden die Downloadraten zunächst bei 2 bis 3 MBit/s in der Empfangsrichtung liegen. In Senderichtung sollen bis zu 5,8 MBit/s möglich sein. Zu HSDPA gehört auch „High Speed Uplink Packet Access" (HSUPA). Beide Verfahren sollen die Datenlast in der Basisstation effektiver verteilen und je nach Qualität der Funkverbindung ein höher verdichtendes Kodierungsverfahren benutzen.

Unternehmen wie Siemens Mobile und Sony Ericsson haben unter Laborbedingungen bereits 14 MBit/s erreicht. Im praktischen Einsatz hält Siemens Mobile eine Rate von 3,6 MBit/s in Empfangsrichtung für realistisch. Derzeit sind über das UMTS-Netz Datenraten von maximal 384 KBit/s möglich.

Für HSDPA wird nicht nur das UMTS-Netz selbst umgerüstet, auch auf die Verbraucher kommt neue Hardware zu: Notebooks oder andere mobile Endgeräte werden eine HSDPA-fähige UMTS-Karte für den PC-Card-Slot benötigen. Und es wird auch neue, HSDPA-fähige Handys geben müssen. Die Hardware wird höchstwahrscheinlich ab Frühjahr 2006 erhältlich sein.

HSDPA und HSUPA sind noch nicht vom 3GPP-Konsortium standardisiert. Ob und wann die Standardisierung kommt, ist noch nicht bekannt. Fest steht jedoch, dass einige Systemausrüster wie Nokia, Siemens und Ericsson mit den Netzbetreibern in Verhandlungen stehen. So soll zumindest HSDPA bis Ende 2005 in die UMTS-Netze implementiert sein.
ZigBee – Funken im Nahbereich Für nicht wenige Experten ist ZigBee so etwas wie ein Geheimtipp, wenn es um die verlässliche, kosteneffektive und besonders stromsparende drahtlose Vernetzung von Sensor- und Steuerungsprodukten, etwa PC-Eingabegeräten,

Basisstation auszutauschen. Basisstation und Handy benutzen jeweils zwei Kanäle im Abstand von 45 oder 95 MHz. Das Handy sendet auf dem tieferen Kanal (Uplink) und empfängt auf dem höheren Kanal (Downlink). Daten lassen sich in GSM-Netzen herkömmlich mit 9,6 KBit/s, per HSCSD mit 14,4 KBit/s (ohne Kanalbündlung) und per GPRS mit bis zu 171 KBit/s übertragen. Der Short Message Service (SMS) erlaubt in GSM-Netzen den Austausch von Kurznachrichten mit bis zu 160 Zeichen Länge, die dann entweder auf dem Handy-Display erscheinen oder von einem PC ausgelesen werden können.

Wegen der relativ geringen Reichweite von nur wenigen Kilometern sind für jedes einzelne Netz in Deutschland mehrere tausend Basisstationen erforderlich. Zur Versorgung funktechnisch schwieriger Gebiete benutzt man so genannte Repeater, etwa für Alpentäler, S-Bahn-Tunnel oder ICE-Züge. Repeater verstärken lediglich die Funksignale und leiten sie von oder zur nächsten Basisstation weiter.

UMTS-Netze (Universal Mobile Telecommunication System) sollen nach und nach die GSM-Netze ergänzen und ablösen. UMTS erlaubt zwei Betriebsarten:

Frequency Division Multiplex (FDD): Das Senden und Empfangen erfolgt wie bei GSM auf unterschiedlichen Frequenzen. Dabei wird eine Datentransfer-Geschwindigkeit bis zu 384 KBit/s erreicht – in beiden Richtungen. FDD ist geeignet für mobilen Betrieb im Umkreis von mehreren Kilometern um jede Basisstation (ähnlich wie GSM). Bei der Einführung von UMTS werden zunächst allerdings maximal 144 KBit/s unterstützt, die tatsächlich nutzbare Netto-Datenrate wird je nach Versorgung bei 20 bis 40 KBit/s liegen.

Time Division Duplex (TDD): Ähnlich wie bei DECT geschieht das Senden und Empfangen auf derselben Frequenz, allerdings zeitlich versetzt. Wegen der kurzen Laufzeit-Toleranz ist TDD jedoch nur für den stationären Betrieb im Nahbereich bis etwa 500 Meter um eine Basisstation geeignet. Die Datenrate von bis zu 2 MBit/s ist allerdings nur für einen Teilnehmer je Basisstation nutzbar. Die Netzbetreiber planen diesen Modus erst für die fernere Zukunft.

Peter Klau

KNOW-HOW

Numerische Präfixe

Einheit	Symbol	Beispiel	Beispiel Symbol	Numerisches Äquivalent
Kilo	k	Kilohertz, Kilobit/Sekunde	KHz KBit/s	1.000
Mega	M	Megahertz Megabits/Sekunde	MHz Mbps	1.000.000
Giga	G	Gigahertz Gigabits/Sekunde	GHz Gbps	1.000.000.000
Tera	T	Terabyte Terahertz	TB THz	1.000.000.000.000
Milli	m	Milliwatt	mW	1/1.000
Mikro	µ	Mikrovolt	µV	1/1.000.000

geht. ZigBee nutzt den zugehörigen IEEE-Standard 802.15.4, der dank automatischer Suche ungenutzter Funkkanäle auch für eine gute Koexistenz mit anderen drahtlosen Netzwerken sorgt.

Daten werden in voreingestellten Zeitintervallen gesendet, zudem wird eine 128-Bit-AES-Verschlüsselung für Datensicherheit unterstützt (auch weitere Verschlüsselungsoptionen stehen zur Verfügung). ZigBee selbst stellt das Protokoll für eine eigene Netzwerkschicht zur Verfügung, die Anwendungssoftware ist in den RAM/ROM-Chips untergebracht. Der Name „ZigBee“ bezieht sich auf den Zickzackflug der Bienen: Denn die Daten suchen sich ihren eigenen Weg von Gerät zu Gerät.

Die ZigBee-Produkte nutzen ebenfalls die freien Frequenzbänder, weltweit wären dies 2,4 GHz, in den USA zusätzlich noch 915 MHz und in Europa 868 MHz. Bei 2,4 GHz können mit zehn Kanälen bis zu 250 KBit/s, bei 915 MHz mit sechs Kanälen bis zu 40 KBit/s und bei 868 MHz mit einem Kanal bis zu 20 KBit/s erzielt werden. Die Reichweite der Produkte liegt – je nach Sendeleistung und Umgebung – zwischen zehn und 75 Metern. ZigBee-Netzwerke können bis zu 255 aktive Knoten pro „Netzwerk-Koordinator“ umfassen, wobei sich mehrere Netzwerk-Koordinatoren verknüpfen lassen (mehr zu ZigBee auf 118).

Nach Erhalt der Daten sinken die ZigBee-Geräte wieder in den Tiefschlaf. Deshalb können sie so stromsparend agieren, dass sie im Batteriebetrieb in Verbindung mit teils stundenlangen Schlafphasen unter Nutzung üblicher Akku-Technik mehrere Monate bis Jahre durchhalten. Bis Ende 2006 sollen weltweit etwa 80 Millionen ZigBee-Geräte im Einsatz sein, vor allem in Privathaushalten.

Near Field Communication Als Sony und Philips Ende 2002 ihre Pläne für eine neue Nahfunktechnik namens Near Field Communication (NFC) vorstellten, sahen manche darin bereits eine Konkurrenz für Bluetooth. Dabei spielt NFC mit 13,56 MHz, einer Übertragungsrate von maximal 424 KBit/s und einer Reichweite von einigen Zentimetern in einer ganz anderen Liga.

Der Datenaustausch startet, indem man etwa einen Bluetooth-PDA und ein passendes Handy für einen Moment unmittelbar nebeneinander hält. Die Geräte identifizieren sich per NFC und starten den Datenaustausch per Bluetooth – und zwar ohne die sonst übliche Funkraum-Suche, Gerätewahl, Dienstewahl und Passwortübergabe. Mastercard und Motorola haben in den USA ein vielbeachtetes NFC-Pilotprojekt gestartet: Dabei kaufen Verbraucher ein, indem sie ihr Handy an ein Lesegerät halten.

Ultra Wideband (UWB) Die UWB-Technik füllt eine Lücke, die Wireless Fidelity (WiFi) bei der Breitband-Übertragung in Home-Netzwerken lässt. Ultra Wideband dient vor allem dazu, Videos kabellos zwischen Geräten wie Camcordern, Fernsehern und Rechnern zu übertragen.

Die UWB-Technik überträgt Video-Streams mit bis zu 480 MBit/s – konkurrierende kabellose Techniken liefern dagegen nur ein bis zehn Prozent dieser Datenrate.

Gegenwärtig ringen die UWB-Entwickler wie das IEEE, die „Multiband OFDM Alliance“ (MBOA) und die „WiMedia-Alliance“ noch um einen gemeinsamen UWB-Standard. Doch zahlreiche Unternehmen warten nicht erst auf eine Einigung, sondern drängen mit neuen Produkten auf den Markt.

Der Verkauf von Ultra-Wideband-fähigen Geräten wird im Jahr 2005 stark anziehen und bis 2008 um jährlich 400 Prozent wachsen. Das sagen jedenfalls renommierte Marktforschungsunternehmen in ihren Untersuchungen voraus.

Protokollfragen

TCP/IP konfigurieren

Nach der Installation des TCP/IP-Protokolls müssen Sie ein paar Einstellungen vornehmen, damit die Computer im W-LAN miteinander kommunizieren können. Unter Windows XP bietet Ihnen der Netzwerkinstallationsassistent seine Hilfe an – aber es ist immer gut, wenn man sich selbst zu helfen weiß.

Das Protokoll TCP/IP verlangt, dass jeder Computer im Netzwerk über eine IP-Adresse verfügt. Diese Adresse besteht aus einer Gruppe von maximal zwölf Ziffern, die durch Punkte voneinander getrennt sind. Kein Computer im Internet oder im lokalen Netzwerk darf die gleiche IP-Adresse besitzen wie ein anderer. Wer sich per Modem ins Internet einwählt, bekommt von seinem Internet-Anbieter bei jedem Verbindungsaufbau eine temporäre IP-Adresse zugewiesen.

In einem lokalen Netzwerk mit TCP/IP lässt sich Windows XP so einstellen, dass einem Computer bei jedem Start automatisch eine IP-Adresse zugewiesen wird. Manche Internet-Software erfordert eine solche „dynamische Adressierung". Dabei ändert sich die IP-Adresse jedesmal, wenn der PC ins Netz geht. Es ist aber auch möglich, jedem Rechner eine feste IP-Adresse im Netzwerk zu geben, also eine „statische Adressierung" vorzunehmen. In diesem Fall startet der Computer immer mit der gleichen IP-Adresse.

Wie IP-Adressen aufgebaut sind

Für ein drahtloses Netzwerk ist es natürlich ebenfalls möglich, feste IP-Adressen zu verwenden oder eine dynamische Adressvergabe zu nutzen.

Eine IP-Adresse besteht aus vier Byte (Oktette genannt), die dezimal dargestellt und durch Punkte getrennt sind, zum Beispiel: 172.31.255.255. Jede Zahl kann einen Wert von 0 bis 255 annehmen. Diese Darstellungsweise dient jedoch nur zur Eingabe beziehungsweise Anzeige. Intern arbeitet der PC dagegen immer mit der dualen Darstellung, also etwa 11000010. 00111110.00001111.00000010. Die Punkte dienen an dieser Stelle lediglich der Orientierung, um die Zuordnung der einzelnen Werte zur „Dotted Decimal Notation" zu erleichtern. Um flexibel zu sein, bezeichnen die beiden ersten Byte den Netzwerk-Teil, die letzten beiden Byte den Host-Teil. Damit lassen sich verschiedene Adressklassen ausdrücken (siehe Kasten).

Und weil nicht zwei Computer die gleiche Adresse haben dürfen, bekommt der Host-Computer bei der Einwahl in das Internet eine dynamische Adresse zugewiesen. Nach dem Beenden der Verbindung kann es sein, dass ein anderer Internet-User diese Adresse erhält. Nur bei einem DSL- oder Kabelmodem-Anschluss ist es möglich, dass der Internet-Provider dafür eine statische IP-Adresse reserviert hat.

Private Adressbereiche nutzen

In einem Wireless LAN müssen Sie die IP-Adressen so verwenden, dass sie nicht mit den im Internet verwendeten in Konflikt geraten. Das ist nicht weiter schwierig, wenn man sich an den Standard für die Vergabe der IP-Adressen hält, der von der „Internet Engineering Task Force" (IETF) entworfen wurde. Nach diesem Standard gibt es drei Bereiche, die nicht als Internet-IP-Adressen verwendet werden dürfen. Aus diesen Bereichen lassen sich die IP-Adressen für ein lokales Netzwerk auswählen. Dabei handelt es sich um die folgenden, privaten IP-Adressbereiche:

10.0.0.0 bis 10.255.255.255 (1 Klasse A-Netz)
172.16.0.0 bis 172.31.255.255 (16 Klasse B-Netze)
192.168.0.0 bis 192.168.255.255 (256 Klasse C-Netze)

Für ein lokales Netzwerk lassen sich beispielsweise alle Adressen nutzen, die mit 192.168.0.0 beginnen. Für jeden weiteren Computer wird der Wert um 1 erhöht (der zweite Computer hätte dann die Adresse 192.168.0.1).

Eine besondere Rolle spielt die Adresse 127.0.0.1: Sie spricht per Definition grundsätzlich den lokalen, eigenen Rechner an. Dieser Adresse wird immer der Name „localhost" zugewiesen. Nach dem Standard der IETF ist die Verwendung des Netzes 127.x.x.x unzulässig; die Adresse 127.0.0.1 kann demnach lediglich dazu genutzt werden, um die Installation des eigenen Rechners zu überprüfen.

Die Subnetzmaske nutzen

Bei IP-Netzen ist es oft sinnvoll, ein Netzwerk in mehrere Teilnetze aufzuteilen. Mit Hilfe der Subnetzmaske kann der Rechner die Zuordnung von Netzwerk-Teil und Host-Teil vornehmen. Sie hat denselben Aufbau wie eine IP-Adresse (32 Bit beziehungsweise 4 Byte). Per Definition sind alle Bit des Netzwerk-Teils auf 1 zu setzen, alle Bit des Host-Teils auf 0.

Ein Rechner, der ein Datenpaket zu einem anderen schicken soll, hat zwei Möglichkeiten: Entweder befindet sich der Empfänger im selben Netzwerk, oder er befindet sich in einem anderen Netz, das durch einen oder mehrere Router mit dem Netzwerk des Absenders verbunden ist.

Der Absender überprüft zunächst die IP-Adresse anhand seiner Subnetzmaske. Ist die Empfängeradresse bekannt, weil sich der Empfänger im selben Netzwerk wie der Absender befindet, werden die Daten sofort abgeschickt. Andernfalls werden die Daten nur dann abgeschickt, wenn dem Absender der Weg zum Empfänger bekannt ist.

IP-Adressen unter XP manuell vergeben

Zum Festlegen der IP-Adressen unter Windows XP folgen Sie diesen Arbeitsschritten:

1. Klicken Sie auf den Start-Button und wählen Sie die Option „Netzwerkumgebung".

2. Klicken Sie auf „Netzwerkverbindungen anzeigen“.
3. Wählen Sie die Verbindung aus, die Sie konfigurieren möchten. Klicken Sie anschließend auf der linken Seite unter „Netzwerkaufgaben“ auf die Option „Die Einstellungen dieser Verbindung ändern“.
4. Bei einer LAN-Verbindung aktivieren Sie die Registerkarte „Allgemein“. Markieren Sie die Option „Internetprotokoll (TCP/IP)“ und klicken Sie auf den Button „Eigenschaften“. Bei einer DFÜ- oder VPN-Verbindung aktivieren Sie die Registerkarte „Netzwerk“. Markieren Sie anschließend per Mausklick die Option „Internetprotokoll (TCP/IP)“ und klicken Sie auf den Button „Eigenschaften“.
5. Klicken Sie auf „IP-Adresse automatisch beziehen“, wenn Sie eine automatische IP-Adressierung wünschen, oder wählen Sie die Option „Folgende IP-Adresse verwenden“, wenn Sie eine statische IP-Adresse verwenden möchten. Geben Sie dann dem Rechner eine feste IP-Adresse, zum Beispiel 192.168.0.1. Verwenden Sie 255.255.255.0 als Subnetzmaske.
6. Klicken Sie auf „OK“ und schließen Sie alle Fenster.

Einen Netzwerk-Client einrichten

Clients, die die Internetverbindungsfreigabe nutzen, müssen so konfiguriert werden, dass sie den Host als Gateway für das Internet verwenden. Unter Windows XP hat der Host intern immer die Adresse 192.168.0.1. Diese Adresse verwenden Sie deshalb als Standard-Gateway. Die Konfiguration eines Clients ist denkbar einfach:
1. Führen Sie die Schritte 1 bis 4 durch, wie sie im letzten Abschnitt beschrieben sind.
2. Möchten Sie einen Client mit einer statischen Adresse einrichten, klicken Sie auf „Folgende IP-Adresse verwenden“. Geben Sie danach die Adressen ein, wie sie in der Abbildung oben rechts auf dieser Seite zu sehen sind.
Sorgen Sie dafür, dass der Host stets hochgefahren ist, bevor die Clients eingeschaltet werden. Andernfalls können diese keine IP-Adresse vom Host empfangen.

SELBSTGEMACHT: Wenn Sie eine statische IP-Adresse verwenden wollen, nehmen Sie die Eintragungen im Fenster „Eigenschaften von Internetprotokoll (TCP/IP“ vor.

3. Beim Verwenden einer statischen Adresse markieren Sie die Option „Folgende DNS-Serveradressen verwenden“ und klicken danach auf „Erweitert“. Aktivieren Sie im nächsten Fenster die Registerkarte „DNS“.
4. Ein Rechner mit der Home-Edition von Windows XP kann keiner Domäne beitreten. Verwenden Sie dagegen Windows XP Professional oder Windows Server 2003, können Sie (durch Kommas getrennt) die DNS-Suffixe festlegen, die zu einem unvollständigen Namen mit einfacher Bezeichnung hinzugefügt werden sollen, bevor eine DNS-Abfrage für diesen Namen weitergeleitet wird. Ein unvollständiger Name mit einfacher Bezeichnung, beispielsweise „amadeus“, enthält keine Punkte. Er unterscheidet sich von einem voll gekennzeichneten Domänennamen, zum Beispiel „amadeus.chip.de“. Ist diese Einstellung aktiviert, müssen Sie mindestens ein Suffix angeben. Ist sie nicht aktiviert, wird sie für keinen Computer angewendet; die Rechner verwenden stattdessen die lokale Konfiguration.
5. Beenden Sie den Vorgang durch das Schließen aller Fenster.

Peter Klau

KNOW-HOW

Die unterschiedlichen IP-Adressklassen

Jede IP-Adresse (Class A bis C) besteht aus einem Netzwerk-Adressanteil (N) und einem Host-Adressanteil (x). Das Unterscheidungskriterium für diese Adressklassen A, B, C, D und E sind die ersten Bits (Most Significant Bit, MSB) der IP-Adresse.

Netz	MSB (bin)	Adressen	Bereich	Bemerkungen
Class A	0	N.x.x.x	0 bis 126. Die Adresse 0.0.0.0 steht für die Default-Route, 127 ist reserviert für das Loopback-Device.	Es existieren genau 126 Class-A-Netze, mit denen man jeweils maximal 16.646.144 Hosts adressieren kann.
Class B	10N.	N.x.x	128 bis 191	Es existieren genau 16.256 Class-B-Netze, mit denen man jeweils maximal 65.024 Hosts adressieren kann.
Class C	110	N.N.N.x	192 bis 223	Es existieren genau 2.080.768 Class-C-Netze, mit denen man jeweils maximal 254 Hosts adressieren kann.
Class D	1110	–	224 bis 239	D-Klasse-Adressen besitzen einen Sonderstatus und werden als Multicast-Adressen meist für die synchrone Datenübertragung (Videokonferenzen, Streaming etc.) verwendet. Eine Trennung in Netzwerk- und Hostanteil gibt es nicht.
Class E	1111	–	240 bis 255	E-Klasse-Adressen stehen im Internet nicht zur Verfügung.

Drahtloser Anschluss unterwegs

Online – immer und überall

Geschäftsreisen können anstrengend und nervig sein – besonders, wenn man nicht das richtige Equipment dabei hat. Denn in anderen Ländern gibt es auch andere Steckdosen und eine abweichende Stromspannung. Doch das ist kein Grund, auf die Kommunikation unterwegs zu verzichten. CHIP sagt Ihnen, worauf Sie achten müssen.

Erfahrene Business-Traveller wissen: Nur mit dem richtigen Equipment ist der Erfolg einer Geschäftsreise garantiert. Immerhin gibt es heute zahlreiche Geräte, die es dem Reisenden ermöglichen, sein Büro in der Westentasche oder im Koffer mitzuführen. Zwar ist das Notebook nach wie vor das wichtigste Utensil auf einer Geschäftsreise, doch gewinnen auch andere mobile Geräte zunehmend an Bedeutung.

Verbindung über Modem und Festnetz

Ob Sie sich im In- oder Ausland aufhalten, eine Verbindung über das Hotelnetzwerk ist zwar die sicherste, aber auch die teuerste Art, im Internet zu surfen. Schon wenige Online-Minuten können die Kosten in astronomische Höhen treiben, auch wenn Ihnen der örtliche Provider Sonderkonditionen einräumt. Erkundigen Sie sich vorher an der Rezeption unbedingt nach den Verbindungskosten.

In jedem Fall preisgünstiger dürfte die Einwahl über den heimischen Provider sein, sofern dieser internationale Einwahlnummern anbietet (siehe **24**). Bei einem längeren Aufenthalt im Ausland ist die Anmeldung bei einem lokalen Internet-Service-Provider eine lohnende Alternative. Wenn Sie vorhaben, mit Ihrem Firmennetzwerk zu kommunizieren, sollten Sie vorher die Wege klären, über die Sie sich dort anmelden können. In den meisten Ländern gibt es beispielsweise keinen ISDN-Anschluss – ein ISDN-Modem können Sie also zuhause lassen.

Trotz unzähliger EU-Richtlinien gibt es keine einheitliche Steckverbindung vom Modem-Kabel des Notebooks zu den landesspezifischen Telefonanschlüssen. Um im Ausland über das Festnetz online zu gehen, brauchen Sie also in den meisten Fällen einen Adapter. Für einen Netzwerkanschluss genügt in Westeuropa und in den USA in der Regel ein Twisted-Pair-Kabel mit einem RJ45-Stecker (Western-Stecker), andere Länder haben jedoch ihre eigenen Normen. Wenn Sie sichergehen wollen, den richtigen Adapter für das Ausland zu besitzen, besorgen Sie sich ein internationales Adapter-Set.

Internet-Cafés oder Hotspots nutzen

Internet-Cafés und Hotspots gibt es inzwischen überall auf der Welt. Dort können Sie sich für einen Bruchteil der Kosten, die für eine Hotel- oder Handy-Verbindung anfallen, per Kabel oder W-LAN ins Internet einwählen. Beim Zugang via W-LAN sind grundsätzlich zwei Verbindungsarten möglich: Gratis-Zugänge und kostenpflichtige Dienste. Während die kostenlosen Zugänge häufig in der Gastronomie anzutreffen sind, finden Sie kostenpflichtige W-LANs beispielsweise auf Flughäfen oder in Hotels. Dabei melden Sie sich über eine Intranet-Portalseite an. Neben dem Internet-Zugang bieten die kostenpflichtigen Zugänge auch lokale Dienste an.

Zum Herstellen der Verbindung nehmen Sie einen mit der entsprechenden drahtlosen Netzwerkkarte ausgestatteten Computer oder PDA im Versorgungsgebiet des Hotspots in Betrieb und stimmen die Kommunikationseinstellungen mit dem Access Point ab. Die weitaus meisten W-LAN-Treiber finden den passenden Kanal automatisch. Auf eine Verschlüsselung wird jedoch weitgehend verzichtet (lesen Sie dazu das Special ab **68**).

Zur Nutzung des Hotspot-Zugangs bekommen Sie an der Hotel-Rezeption oder beim Hotspot-Betreiber eine Access-Card mit den notwendigen Angaben zur Zugangsprozedur sowie einen Benutzernamen und Passwort. Dadurch wird die Nutzung des Access Points für einen bestimmten Zeitraum möglich. Über den Web-Browser rufen Sie die Zugangsseite des Hotspots auf und geben die Zugangsdaten ein.

Location Based Services: Jeder Reisende weiß – in einer fremden Stadt geht es nicht ohne die Hilfe Ortskundiger. Der Weg zum nächsten Geldautomaten, zur nächsten Apotheke oder zur Edel-Pizzeria ist allein nur schwerlich zu finden. Doch inzwischen können Sie Ihren Computer oder Ihr Handy um Rat fragen. Denn ortsbezogene Dienste, so genannte „Location Based Services“ (LBS), bieten W-LAN-Usern und Handy-Nutzern Informationen, die speziell auf ihren aktuellen Aufenthaltsort zugeschnitten sind.

Sicherheit von Hot Spots: Hotspots arbeiten als offene Funknetze, eine Datenverschlüsselung gibt es aus praktischen Gründen

AB INS INTERNET: Nachdem Sie sich die Access Card besorgt haben, geben Sie nur noch Benutzername und Passwort ein.

Die besten Online-Zugang-Tipps im Web

Kosten im Blickfeld → www.tariftip.de
Tipps zu internationalen Internet-Zugängen und Tarifen
Internet-Cafés → www.net-cafes.com
Globale Suchmaschine für Internet-Cafés
Immer Anschluss → www.ime.de, www.targus.com
Anbieter von internationalen Adapter-Sets
Hotels mit W-LAN → www.wlan-germany.com
Aufstellung aller W-LAN-Hotels in Deutschland

selten oder nie. Schließlich soll dem Nutzer das Abtippen langer WEP-Schlüssel und eine komplizierte Konfiguration erspart werden. Für die Sicherheit Ihrer Daten sind Sie also selbst verantwortlich. Denken Sie daran: Sämtliche Daten, die Sie über ein nicht gesichertes Funknetz senden, sind von anderen lesbar – wenn auch mit einigem Aufwand. Wenn Sie das beachten und beim Austausch sensibler Daten zurückhaltend sind, steht Ihrem W-LAN-Vergnügen nichts mehr im Weg.

Sicherheit im Internet-Café: Die Online-Verbindung über ein Internet-Café erfordert den geringsten technischen Aufwand. Doch insbesondere im Umgang mit öffentlichen Computern sollten Sie wachsam sein in Bezug auf sensible Daten wie Passwörter für E-Mail-Accounts oder Online-Banking. Auf diese Punkte sollten Sie besonders achten:

Deaktivieren Sie die Funktion der Auto-Vervollständigung, also das Merken von Passwörtern und Internet-Adressen durch den Browser. Prägen Sie sich die nötigen Schritte vor Reiseantritt ein, denn der Internet-Browser wird im Ausland in der Landessprache betrieben.

Verzichten Sie in einem Internet-Café auf Online-Banking.

Mit der Tastenkombination [Strg]+[H] können Sie eine Liste der zuletzt besuchten Seiten, die „History", aufrufen und löschen. Falls die Tastenkombination nicht funktioniert, finden Sie die Liste unter Begriffen wie „History" oder „Verlauf".

Vorsicht: Teure Roaming-Gebühren beim Handy

Mit dem Handy im Ausland eine Verbindung aufzubauen, ist technisch recht einfach. Schwieriger wird es, im Tarifdickicht das preisgünstigste Angebot zu ermitteln. Das Telefon findet zwar leicht ein verfügbares Netz, die Roaming-Gebühren machen aber oft schon die Übertragung von ein paar hundert KByte zu einer kostspieligen Angelegenheit. In der Regel ist es günstiger, ein Mobilgerät von einem Anbieter vor Ort zu mieten. Viele Provider locken mit günstigen Pauschaltarifen und einem Guthaben. Wer im Ausland viel telefonieren muss, ist mit einer Prepaid-Karte eines lokalen Providers gut beraten.

Besonders moderne Handys verfügen nicht selten über ein integriertes E-Mail-Programm. Damit schreiben und empfangen Sie E-Mails in der Regel zu günstigeren Preisen als mit einem Notebook oder PDA, weil weniger Online-Zeit benötigt wird. Und schließlich: Die gute alte SMS kostet – im Ausland abgeschickt – nur das Zwei- bis Dreifache von dem, was in Deutschland zu bezahlen ist.

Mobilfunkbetreiber wie T-Mobile, Vodafone, D2, E-Plus und O2 bieten als besonderen Service an, E-Mails per SMS zu empfangen beziehungsweise zu verschicken. Das Problem dabei ist die für SMS übliche Beschränkung auf 160 Zeichen. Das bedeutet: Beim Schreiben einer Nachricht müssen Sie sich auf das wesentliche konzentrieren. Nähere Informationen erhalten Sie von den Mobilfunkbetreibern unter dem Stichwort „SMS".

Einfacher und ohne Zeichenbeschränkung ist das Senden und Empfangen von E-Mail via WAP. Dazu benötigen Sie einen Provider, der WAP-Mails anbietet. Das Übertragen von WAP-Mails ist allerdings nicht ganz billig. Nähere Auskunft erhalten Sie auf der Website der einzelnen Internet-Provider unter dem Stichwort „WAP".

Fast alle Mobiltelefone bieten für das Notebook oder den PDA Anschlussmöglichkeiten über Kabel, Bluetooth oder Infrarot. Wenn eine Empfangsmöglichkeit besteht, ist auf diese Weise auch das Internet erreichbar. Diese Verbindung ist meistens langsamer als per Kabel, trotzdem sind die Kosten hoch. Dennoch kann diese Konfiguration preiswerter sein als das →

PROFI-TIPPS

Checkliste fürs mobile Büro

Wer viel unterwegs ist, sollte auf jeden Fall sein Reisegepäck optimieren. Nichts ist frustrierender, als in einer fremden Stadt festzustellen, dass man ein wichtiges Teil seiner IT-Ausrüstung vergessen hat. Sie reisen also wesentlich entspannter, wenn Sie die folgende Checkliste genau beachten.

Zweites Stromkabel und Ladegerät für das Notebook besorgen. Dadurch bleibt Ihre Büro-Konfiguration erhalten.

Euro-Stecker und internationales Adapter-Set sind unerlässlich.

Transformator Ihr Notebook sollte mit einer Netzspannung von 100 bis 250 Volt bei einer Frequenz von 50 und 60 Hz arbeiten. Andernfalls ist ein Transformator erforderlich, der die Spannung anpasst. Diese Geräte sind im Fachhandel erhältlich, einige Notebooks enthalten aber bereits einen Spannungswandler.

Modem Ein W-LAN-, ISDN- oder DSL-Anschluss steht Ihnen im Ausland eventuell nicht zur Verfügung.

W-LAN-Netzwerkkarte mitnehmen. Unzählige Hotspots auf der ganzen Welt ermöglichen Ihnen das Einloggen. Einige Hotspots unterstützen darüber hinaus Bluetooth.

Twisted-Pair-Kabel Ein aufrollbares Twisted-Pair-Netzwerkkabel sollte nicht fehlen. Mit einer Länge von fünf Metern erreichen Sie die meisten Anschlussdosen im Hotel oder Konferenzraum.

CD-R-Rohlinge in die Tasche packen. Schließlich gibt es immer etwas zu kopieren (Präsentationen, Multimedia-Dateien etc.).

USB-Stick besorgen. Damit gestaltet sich der Datenaustausch besonders bequem.

Drahtlose oder USB-Maus erleichtert die Arbeit mit dem Notebook erheblich.

Headphone für das Handy Sie sind zwar etwas sperrig, aber sie funktionieren – und kein lästiger Zeitgenosse wird Sie ansprechen, solange Sie so ein Ding tragen.

USB-Licht Diese Lichtquelle hilft Ihnen in abgedunkelten Hotelzimmern oder bei einem Langstreckenflug.

Frische Batterien oder Akkus einpacken. So können Sie auf längeren Flügen arbeiten oder DVDs ansehen. Vergessen Sie auch das Ladegerät für die Akkus nicht.

Backup-CDs Installations- oder Backup-CDs sind die Lebensversicherung für Ihr Betriebssystem und wichtige Applikationen. Vergessen Sie auch nicht die VPN- oder Einwahlsoftware; andernfalls kann die Kommunikation ziemlich kompliziert und teuer werden.

hoteleigene Netzwerk. Fragen Sie vor der Reise Ihren Mobilfunk-Anbieter nach den Möglichkeiten und Preisen. Techniken wie GPRS erlauben höhere Übertragungsraten und eine genauere Abrechnung. Die erfolgt bei GPRS nach dem Datenvolumen und nicht nach der Verbindungszeit.

Für die Mobilfunkbetreiber könnten sich die standortbezogenen Dienste (LBS) zu einer neuen Schlüsselapplikation entwickeln, die besonders dem UMTS-Netz zum Erfolg verhelfen kann. Technische Grundlage dieser Dienste ist die Möglichkeit, ein eingeschaltetes Handy zu lokalisieren. Die Ortsbestimmung erfolgt über die gesprächsführende Mobilfunkzelle, wobei die Größe der Funkzelle variabel ist und unter anderem von der geographischen Beschaffenheit und der Dichte des Mobilfunkbetriebs abhängt. Daher sind die Funkzellen in Städten wesentlich kleiner als in ländlichen Gebieten, sodass sich die Position eines Nutzers in City-Lagen bis auf wenige hundert Meter genau bestimmen lässt. In ländlichen Gebieten, wo die Lokalisierung der Nutzer nicht so genau erfolgen kann, bieten sich standortbezogene Dienste daher kaum an.

Internet-Einwahl über heimische Provider

Selbst wenn Sie rund um den Globus unterwegs sind, brauchen Sie nicht auf die gewohnte Einwahl bei Ihrem Internet-Anbieter zu verzichten. Allerdings bieten nur wenige große deutsche Provider eine Einwahl im Ausland an. Im Zweifelsfall finden Sie auf der Homepage Ihres Anbieters Informationen darüber. Relativ kostengünstig gestaltet sich die Einwahl im Ausland bei den Internet-Diensten von T-Online und AOL:

Als T-Online-Kunde wählen Sie mit der Zugangs-Software das jeweilige Land aus und registrieren sich auf der Homepage für den Dienst. Die Anmeldung ist kostenlos und es fällt auch keine Grundgebühr an. Für das Nutzungsentgelt ist die Welt in vier Tarifgebiete aufgeteilt. Im Schmalbandbereich kostet die Surf-Minute zwischen vier und 16 Cent. Der Zugang ist jedoch auch über DSL und WLAN möglich: Hier werden pro Minute zwischen 16 und 32 Cent berechnet. Diese schnellen Internet-Zugänge stehen aber nicht in allen Ländern zur Verfügung. Informationen zum internationalen Zugang mit T-Online finden Sie unter **www.service.t-online.de**.

Sind Sie AOL-Kunde, wählen Sie ebenfalls mit Hilfe der Zugangs-Software das Land aus, in dem Sie sich aufhalten werden. Der Dienst funktioniert ganz einfach über die normale AOL-Software ab Version 6.0. Es entstehen keine zusätzlichen Kosten, da die Einwahl direkt ins AOL-Netz erfolgt. Mehr Infomationen bekommen Sie unter der Adresse **www.aol.de/zugang**.

Internet-Zugang über Roaming-Dienste

Spezielle Dienstleister wie Ipass (**http://de.ipass.com**) bieten für Geschäftsreisende preisgünstige lokale Einwahlknoten an.

Über mehr als 22.000 Einwahlpunkte in über 140 Ländern der Erde verfügt das englische Unternehmen Net2roam. Die Nutzungsdauer lässt sich der Reiselänge anpassen. Net2Roam arbeitet mit der GIRC-Plattform, zu der sich Provider weltweit zusammengeschlossen haben. Pro Minute werden acht US-Cent fällig. Weitere Informationen bekommen Sie im Internet unter der Adresse **www.net2roam.com**.

Eher an Geschäftsleute, die jederzeit und möglichst überall auf das Internet zugreifen wollen, wendet sich die Mobile Connect Card von Vodafone. Sie ersetzt die Verbindung über das Handy. Sie schieben einfach die Karte ein und legen los. Das Surfen per PC-Datenkarte ist allerdings sehr teuer: Neben dem hohen Preis der Mobile Connect Card von mindestens 200 Euro treibt GPRS die Kosten in die Höhe. Dazu kommen im Ausland die Gebühren für die Roaming-Partner. Mehr Informationen bekommen Sie unter: **www.vodafone.de/mobil_ausland**.

Bei allen Anbietern kommen die Gebühren für die Telefonverbindung dazu, und die können in Hotels bekanntlich sehr hoch sein. Welche Zugangsart Sie auch wählen, führen Sie vorher mit dem Hotelmanager ein klärendes Gespräch über die zu erwartenden Kosten. Bei einem längeren Auslandsaufenthalt lohnt sich die Anmeldung bei einem lokalen Provider. Kleiner Tipp: Aufgrund der zentralen Abrechnung können Firmen mit hohem Reiseaufkommen mit verschiedenen Hotelketten individuelle Rahmenverträge abschließen. Die Anmeldung an den Hotspots aller kooperierenden Hotels erfolgt dann mit einem persönlichen Zugangscode, die Abrechnung monatlich über das von allen Mitarbeitern verbrauchte Datenvolumen oder die Gesamtnutzungsdauer.

Peter Klau

KNOW-HOW

Mobilfunknetze und W-LAN im Vergleich

Eigenschaften	802.11g	802.11b	UMTS	GPRS	GPM
Max. Reichweite	300 Meter	550 Meter	20 Kilometer	20 Kilometer	30 Kilometer
Übertragungsrate maximal	54 MBit/s	11 MBit/s	2 MBit/s	115 KBit/s	9,6 KBit/s
realistisch	25 bis 30 MBit/s	4 bis 6 MBit/s	144 KBit/s	40 KBit/s	6 KBit/s
Frequenzbereich	5000 MHz	2400 MHz	2000 MHz	900, 1800, 1900 MHz	900, 1800, 1900 MHz
Flächendeckung	Hotspots	Hotspots	Ballungsgebiete, Großstädte	Flächendeckend	Flächendeckend
Roaming	Zellenwechsel: vereinzelt National: nein International: nein		Zellenwechsel: ja National: ja International: ja		
Mobilität	Sehr eingeschränkt (bis 10 km/h)		Hoch		
Authentifikation	Login-Prozedur, zusätzliche Hardware		Ja		

Wireless Fidelity

Leben und arbeiten mit WiFi

Unter Wireless Fidelity (WiFi) versteht man eine funkgestützte LAN-Kommunikation zwischen Notebooks, Handhelds und stationären Computern. WiFi-Geräte sind handlich, schnell und haben eine Reichweite von etwa 30 Metern. Man trifft sie immer häufiger auf Flughäfen, in Hotels und in Coffee-Shops.

Vielleicht erinnern Sie sich noch an die erste Reise ins Ausland, auf der Sie vergeblich versucht haben, das Modem-Kabel Ihres Notebooks mit der Telefonanschlussdose zu verbinden, um Ihre E-Mails abzurufen. Entweder war das Kabel zu kurz oder der Stecker inkompatibel. Glücklicherweise sind diese Zeiten inzwischen vorbei. An öffentlichen Einwahlpunkten (Hotspots) stellen Sie drahtlos und ohne Frusterlebnisse eine Verbindung ins Internet her.

Internet, wo Sie es brauchen

Der Begriff „Hotspot" gehört wohl zu den populärsten in der Netzwerktechnik. Bei W-LANs und Bluetooth versteht man darunter einen Knotenpunkt in einem drahtlosen Netzwerk, von dem aus man auf ein Netzwerk zugreifen kann. Es handelt sich um einen räumlich begrenzten Funkbereich, der auf einen Raum, eine Halle oder eine Produktionsstätte begrenzt sein kann. Hotspots, wie man sie in Hotels, Flughäfen, Messehallen, Waschsalons, Bahnhöfen oder Kongresszentren findet, bieten außerdem ortsbezogene Dienste an, auch Location Based Services (LBS) genannt. Bei diesen ortsbezogenen Diensten handelt es sich um maßgeschneiderte Dienstleistungen und Informationen, vor allem um Reisedienstleistungen, Routenplaner, City-Guides, Fahrpläne sowie Point-of-Interest-Ortung.

Vor allem Geschäftsreisende benutzen Hotspots als Zugang zum „Mobile Office". Die drahtlose Technik ermöglicht den Zugang zum Internet und somit die Nutzung aller im globalen Netz verfügbaren Anwendungen und Dienste. Auch der Zugriff auf das firmeneigene Intranet ist auf diese Weise möglich. Auf diese Weise lassen sich die Wartezeiten im Hotel, auf Bahnhöfen oder Flughäfen produktiv nutzen.

Während man mit dem Handy auch auf der „grünen Wiese" eine Online-Verbindung herstellen kann (sofern dort der Empfang möglich ist), ist man beim W-LAN auf einen Hotspot angewiesen. Grundvoraussetzung für die Nutzung eines Hotspots sind ein mobiles Endgerät mit einer W-LAN-Netzwerkkarte und ein Internet-Browser.

CHIP → DVD-CODE W-LAN

→ **Netzwerke aufspüren** Der Network Stumbler erlaubt es Ihnen zum Beispiel, drahtlose Netzwerke aufzuspüren, Antennen optimal auszurichten oder Versorgungslücken in Ihrem eigenen Netzwerk zu finden. Das Tool stellt fest, ob andere WLANs möglichweise Ihr eigenes Netz stören, oder ob unauthorisierte Nutzer versuchen, sich einzuloggen.

WiFi – ein Blick in die nahe Zukunft

Von großem Interesse sind auch WiFi-Implementationen, die einen merklich größeren Bereich versorgen. In diesem Zusammenhang haben sich zwei Verfahren herauskristallisiert, die verschiedene geographische Bereiche abdecken: WiFi-Zonen und WiFi-Wolken.

Eine WiFi-Zone besteht aus einem Zusammenschluss verschiedener Hotspots, die ein gemeinsames Managementsystem benutzen. Nach der Anmeldung mit Benutzernamen und Kennwort ist es dem WiFi-Anwender in dem geographischen Gebiet, das von der Zone abgedeckt wird, möglich, an beliebiger Stelle auf das Netzwerk zuzugreifen. Eine WiFi-Zone kann zum Beispiel ein großes Areal wie ein Einkaufszentrum oder eine Industriemesse abdecken. Das Gebiet, das als WiFi-Zone definiert ist, muss dabei nicht einmal zusammenhängend sein. Eine solche Zone kann auch aus zwei Hotspots an den gegenüberliegenden Grenzen einer Stadt bestehen, mit großen Versorgungslücken dazwischen. Das Gemeinsame sind in diesem Fall die angebotenen Dienste und nicht die geographische Lage.

WiFi-Wolken bieten eine kontinuierliche Flächendeckung über einem bedeutenden Teil einer Stadt oder über einem bestimmten geographischen Gebiet. Die Wolken bestehen aus multiplen Hotspots, die im Gegensatz zu einer Zone ein zusammenhängendes Areal abdecken. Die Größe einer WiFi-Wolke kann stark variieren, wichtig ist die lückenlose Flächendeckung.

Via Hotspot ins Internet

Die Verbindung ins Internet über einen Hotspot ist recht einfach aufgebaut – dank Wireless LAN und dem zugehörigen Standard IEEE 802.11b. Allerdings müssen Sie vor der drahtlosen Einwahl ins Internet ein paar Einstellungen ändern. Die Zugangsdaten erhalten Sie vom Hotspot-Anbieter, auch Wireless Internet Service Provider (WISP) genannt. Die folgenden Schritte verhelfen Ihnen zu einem stressfreien Hotspot-Zugang.

1. Die WLAN-Einstellungen anpassen

Öffnen Sie die „Netzwerkverbindungen" innerhalb der Systemsteuerung von Windows XP. An dieser Stelle ist auch Ihre drahtlose W-LAN-Verbindung aufgeführt. Klicken Sie mit der rechten Maustaste auf das zugehörige Symbol und wählen Sie die Option „Eigenschaften". Anschließend klicken Sie auf den Button „Konfigurieren", der zum W-LAN-Adapter gehört. Auf

Die besten Hotspot-Tipps im Web

Suche nach Hotspots → www.nodedb.com
Das Wireless-Node-Datenbank-Projekt listet Hotspots weltweit
Deutsches Hotspot-Verzeichnis → mobileaccess.de/wlan/
Hotspots suchen und melden, technische Hilfe, Newsletter...
WiFi-Zonen-Katalog → www.wifizone.org
Globales, detailliertes Verzeichnis von WiFi-Zonen
Hotspots in Magenta → 80.146.239.232/tcomhsl
Hier finden Sie alle Hotspots von T-Com und T-Mobile

der Registerkarte „Erweitert“ finden Sie sämtliche Einstellungen, die für den Internet-Zugang via Hotspot wichtig sind. Auf die folgenden Optionen müssen Sie achten:

Channel: Gibt der Wireless Provider (WISP) einen speziellen Kanal vor, auf dem gesendet wird, können Sie ihn an dieser Stelle auswählen.

Encryption: Manche WISP arbeiten mit deaktivierter WEP-Verschlüsselung. In diesem Fall müssen Sie diesen Wert auf „disabled“ stellen. Damit trotzdem ein Höchstmaß an Sicherheit garantiert bleibt, sollten Sie Security-Tools wie VPN (Virtual Private Network) oder Verschlüsselungssoftware benutzen.

Network Type: Der W-LAN-Standard IEEE 802.11 kennt zwei Netzwerk-Betriebsmodi: Ad-hoc und Infrastruktur. Für den Zugang via Hotspot muss „Infrastructure“ eingestellt sein.

SSID: Tragen Sie an dieser Stelle die Kennung des Hotspots ein, die vom Provider des drahtlosen Einwahlpunkts zur Verfügung gestellt wird. Oft funktioniert auch die Einstellung „any“.

2. Die IP-Adresse automatisch beziehen

Innerhalb der Eigenschaften der drahtlosen Netzwerkverbindung muss das Netzwerkprotokoll TCP/IP installiert und wie folgt konfiguriert sein:

Die Einstellungen „IP-Adresse automatisch beziehen“ und „DNS-Serveradresse automatisch beziehen“ müssen aktiviert sein. Klicken Sie außerdem auf „Erweitert“ und stellen Sie sicher, dass „DHCP aktiviert“ eingestellt und die Liste „Gateway“ leer ist.

Damit Ihr W-LAN-Adapter eine neue gültige IP-Adresse des Hotspot-Providers erhält, klicken Sie mit der rechten Maustaste auf die drahtlose Netzwerkverbindung. Wählen Sie anschließend die Option „Reparieren“.

3. Den Proxy ausschalten

Wenn Sie via Hotspot ins Internet gehen wollen, benötigen Sie keinen Proxy-Server. So schalten Sie ihn aus:

W-LAN-HOTSPOTS: Für schnelle Hotspot-Suche eignen sich spezielle Suchmaschinen, beispielsweise auf www.portel.de.

PROFI-TIPPS

Was Sie zu WiFi wissen müssen

Windows sicherer machen
Fast alle fernsteuerbaren Windows-Dienste laufen über den so genannten Server-Dienst. Die meisten W-LAN-Nutzer brauchen diesen Dienst nicht und können ihn einfach abschalten. Dazu wählen Sie im Ordner „Verwaltung“ das Modul „Dienste“ und dort den Dienst „Server“. Ändern Sie seinen Status auf „Deaktiviert“. Dies funktioniert mit einem Rechtsklick auf den Dienst und die Wahl von „Eigenschaften | Starttyp“. Ohne Server-Dienst kann sich niemand über das Netz auf Ihrem Notebook anmelden, auf Dateien zugreifen oder sogar Programme starten.

Surfen auf höchstem Niveau
Lufthansa bietet Ihnen mit FlyNet als weltweit erste Airline einen W-LAN-Internet-Zugang mit einem eigenen, kostenlosen Service-Portal. Damit können Sie nun auf Langstreckenflügen all das erledigen, wozu Ihnen bislang am Boden die Zeit oder in der Luft die Möglichkeiten fehlten. Info: www.flynet.lufthansa.com

W-LAN-Finder für die Tasche
Wenn Sie auf der Suche nach dem nächstgelegenen W-LAN-Hotspot sind und dabei nicht ständig mit einem aufgeklappten Notebook oder einem W-LAN-fähigen Endgerät unterwegs sein wollen, brauchen Sie einen W-LAN-Finder. Diese Geräte gibt es bereits im Kreditkartenformat. Für den Betrieb sind weder ein Computeranschluss noch irgendeine Software erforderlich. Auf Knopfdruck teilt Ihnen der W-LAN-Finder mit, ob es im Umkreis von 60 Metern W-LAN-Aktivitäten gibt. Je mehr LEDs aufleuchten, um so stärker ist das Funksignal. Der W-LAN-Finder erkennt und misst sowohl 802.11b- als auch 802.11g-Signale. Signale von drahtlosen Telefonen, Mikrowellen und Bluetooth-Netzen filtert das Gerät aus, sodass keine Falschmeldungen auftreten. Der W-LAN-Finder ist im Handel für etwa 33 Euro erhältlich. Infos: www.arp-datacon.de

Spotfinder Mit dem Spotfinder finden Sie W-LAN-Hotspots online ebenso wie offline. Damit erleichtert Ihnen das Tool das mobile Arbeiten und Sie können die Vorteile von Wireless LAN voll nutzen. Das Programm zeigt Ihnen, wo Sie sich am schnellsten kostenlos oder kostenpflichtig ins Internet einklinken (Freeware für Windows XP, Windows 9x, Windows Me, Windows 2000/NT). Infos und Download: www.netsale.ch/netsale/spotfinder

Internet Explorer Öffnen Sie das Menü „Extras“ und wählen Sie die Option „Internetoptionen“. Dort aktivieren Sie die Registerkarte „Verbindungen“ und klicken auf die „Einstellungen“, die zu Ihrem LAN gehören. Deaktivieren Sie per Mausklick den Proxyserver, falls einer eingestellt sein sollte. Das beeinträchtigt nicht die Sicherheit des drahtlosen Internet-Zugangs, da Hotspots ohne Proxy betrieben werden. Falls Sie sich via Hotspot in Ihr Firmennetzwerk einwählen wollen, sollten Sie selbst für die notwendige Sicherheit sorgen, beispielsweise mit einer sicheren VPN-Verbindung.

Netscape Navigator Unter „Bearbeiten | Einstellungen“ wählen Sie den Menüpunkt „Erweitert“. Klicken Sie zweimal auf „Proxies“ und deaktivieren Sie anschließend „manuelle“ oder „automatische Proxy-Konfiguration“.

Opera Unter „Datei | Einstellungen“ finden Sie die Option „Netzwerk“. Klicken Sie auf „Proxy Server…“ und deaktivieren Sie einfach alle vorhandenen Felder.

Peter Klau

Drahtlos im Nahbereich

Funknetz mit Bluetooth

Auf dem Sofa E-Mails abschicken und im Garten im Internet surfen? Kein Problem. Mit Bluetooth können PCs und Notebooks kabellos auf das Internet zugreifen. Aber auch bei spontanen, temporären Vernetzungen oder im Zusammenspiel mit Handys, Druckern und PDAs kommt dieser Funkstandard immer öfter ins Spiel.

Mit Bluetooth können Sie eine Vielzahl mobiler Endgeräte in kurzer Zeit kabellos, schnell und komfortabel miteinander verbinden. Die Technik wurde bereits 1994 von der schwedischen Firma Ericsson entwickelt. Zur weltweiten Durchsetzung dieser Technologie gründeten Unternehmen wie Ericsson, IBM, Nokia und Intel die „Bluetooth Special Interest Group" (SIG), eine Interessengemeinschaft, die die offene, nicht mit Lizenzgebühren belegte Spezifikation „Bluetooth" weiterentwickelte. Der Name Bluetooth erinnert an den mittelalterlichen dänischen Wikingerkönig Harald Blatland (wörtlich: Blauzahn), der zwischen 910 und 986 große Teile Skandinaviens in seinem Reich vereinte.

Ein wesentliches Ziel von Bluetooth besteht in dem Ersatz der bestehenden Kabelverbindungen, denn oft ist aufgrund inkompatibler mechanischer Kabelverbindungen ein Datenaustausch zwischen unterschiedlichen Geräten nicht möglich. Ein weiterer Vorteil ist der praktisch selbstständige Verbindungsaufbau der Geräte miteinander. Bei Bluetooth handelt es sich um eine plattformübergreifende Technologie, sie kann also in den verschiedensten elektronischen Geräten eingesetzt werden. Mehrere hundert Hersteller setzen bereits auf diese Technik, ohne dass bisher irgendwelche Kompatibilitätsprobleme aufgetreten sind.

So funktioniert Bluetooth

Mit Bluetooth lassen sich Notebooks, Mobiltelefone, Headsets, PDAs, Digitalkameras und Telefone miteinander oder über einen Access Point verbinden. Die gegenseitige Identifizierung der einzelnen Bluetooth-Geräte erfolgt durch eine weltweit eindeutige Adresse von 48 Bit Länge (ähnlich wie die MAC-Adresse im Ethernet-Netzwerk); dies ermöglicht die Vergabe von 281 Billionen Adressen. Bluetooth arbeitet in einem Frequenzbereich zwischen 2,402 und 2,480 GHz, dem ISM-Band (Industrial, Scientific, Medical), das weltweit frei und unlizenziert zur Verfügung steht.

Der Stromverbrauch der Bluetooth-Geräte während einer Verbindung ist so gering, dass die Technologie auch in batteriegetriebenen Geräten zum Einsatz kommen kann. Miteinander verbundene Bluetooth-Geräte erreichen eine Übertragungsgeschwindigkeit von einem MBit/Sekunde Datendurchsatz (brutto). Die Netto-Datenübertragung einer Bluetooth-Verbindung beträgt in der Regel 723 KBit/s in Richtung Verbraucher und 57,6 KBit/s in der Gegenrichtung. Bei symmetrischer Übertragung sind es 432,6 KBit/s pro Richtung, also 865,2 KBit/s insgesamt. Mit diesen Werten erreicht die asymmetrische Download-Geschwindigkeit von 723,2 KBit/s nahezu die typische DSL-Geschwindigkeit. Einige Bluetooth-Profile, beispielsweise PAN (siehe Kasten auf 30), ermöglichen außerdem das Aushandeln von Kompressionsverfahren, sodass ein effektiver Datendurchsatz sogar bis in den MBit/s-Bereich möglich ist.

KNOW-HOW

Bluetooth-Steckbrief

Sendefrequenz: 2,4 GHz im lizenzfreien ISM-Band (Industrial, Scientific, Medical)
Sendeleistung: 1 bis 100 mW je nach Klasse, damit Reichweiten von fünf bis 50 Meter
Sicherheit: 128-Bit-Verschlüsselung
Kanäle: Wechselt bis zu 1.600mal pro Sekunde zwischen über 70 Frequenzen (Frequency-Hopping)
Maximale Brutto-Datenrate: 1 MBit/s (0,7 MBit/s Nutzdaten)
Maximale Anzahl der Kommunikationspartner: 256, davon maximal acht gleichzeitig in einem Pico-Netz aktiv
Wichtigster Einsatzbereich: Übertragung von Daten und Sprache zwischen mobilen Endgeräten im Nahbereich

So weit können Sie mit Bluetooth funken

Die Bluetooth-Technologie ermöglicht also eine kostengünstige, drahtlose Funkverbindung mit niedrigem Stromverbrauch und kurzer Reichweite. In der Standardausführung beträgt die maximale Reichweite zehn Meter – der größte Abstand, über den eine Verbindung aufrechterhalten werden kann. Einige Bluetooth-Geräte verfügen allerdings über stärkere kombinierte Sender-Empfänger, was sehr wahrscheinlich größere Reichweiten ermöglicht. Die Sendeleistung hängt außerdem von der Gebäudebauweise und äußeren Störeinflüssen ab.

Nach der Bluetooth-Spezifikation sind derzeit drei Sendeleistungsklassen möglich. Sie unterscheiden sich in der Sendeleistung (Reichweite) und damit auch im Energieverbrauch (siehe Kasten auf 31): Die Abkürzung „dBm" bezeichnet einen Signalpegel, bezogen auf die Leistung von 1 Milliwatt

CHIP → DVD-CODE W-LAN

→ **Bluetooth-Schnüffler** Auf DVD finden Sie das W-LAN-Sniffing-Tool iStumbler für den Mac. Die Software erkennt nicht nur WiFi-Geräte, sondern auch Bluetooth-Verbindungen. Über das Bluetooth-Plugin lassen sich Informationen zu den erkannten Geräten anzeigen, der Dateiinhalt des Gerätes durchforsten und Dateien versenden.

Die besten Bluetooth-Tipps im Web

Hardware-Katalog → www.bluetooth-db.de
Eine Übersicht über aktuelle Bluetooth-Geräte inklusive Ergebnissen von Kompatibilitätsprüfungen liefert die Bluetooth-Datenbank
Know-how ohne Ende → www.palowireless.com
Der ultimative Internet-Guide für drahtlose Technologien
Support → www.bluetooth.com, german.bluetooth.com
Die offizielle Info-Website in Englisch und Deutsch

(mW) im logarithmischen Maßstab. In der elektrischen Nachrichtentechnik werden die Leistungen von Signalen fast ausschließlich in dBm angegeben.

Um die begrenzten Energiereserven in mobilen Endgeräten wie Mobiltelefonen oder PDAs zu schonen, kommt in den meisten Fällen die Klasse-3-Variante mit 0 dBm = 0,001 Watt = 1mW zum Einsatz.

Der Bluetooth-Standard sieht vor, dass die leistungsgeregelte Sendeleistung nur den jeweils erforderlichen Wert annehmen soll. Verbessert sich die Empfangsqualität, etwa wenn sich die Entfernung zwischen Sender und Empfänger verringert, wird weniger Sendeleistung benötigt. Daraufhin wird die Sendeleistung reduziert, sodass der Stromverbrauch und auch die elektromagnetische Emission sinken. Dieser Modus muss nicht, kann aber in einem Bluetooth-Modul der Klasse 3 – dem Standard entsprechend – realisiert sein.

Bluetooth-Signale werden auf unterschiedlichen Frequenzen, jedoch mit konstanter Leistung abgestrahlt. Berücksichtigt man, dass die Kanalumschaltezeit zum Sprung in den nächsten Frequenzbereich 0,220 Millisekunden dauert, wird die Sendeleistung während nur 0,405 Millisekunden (0,625 minus 0,220 Millisekunden) und das 1.600mal pro Sekunde abgestrahlt. Die Spitzensendeleistung sollte daher mit dem Faktor 0,65 (0,405 geteilt durch 0,625 Millisekunden) auf die mittlere Sendeleistung umgerechnet werden.

Wer Bluetooth dazwischenfunken kann

Dank des schnellen Frequenzwechsels (Frequency-Hopping) zwischen 79 Funkkanälen können Bluetooth-Geräte automatisch zur zuverlässigsten Frequenz wechseln und somit für eine bessere und schnellere Übertragung sorgen.

Trotzdem sind Störungen möglich. Häusliche Mikrowellen, Diathermie-Anwendungen (Durchwärmungsbehandlung mit hochfrequentem Wechselstrom), Fernsehüberwachung, Funksteuerungsanlagen oder auch ein Wireless LAN nach dem Standard IEEE 802.11b teilen sich mit Bluetooth das ISM-Band. Bei einem gemeinsamen Einsatz von Wireless LAN und Bluetooth ist eine Störung zu Lasten von Bluetooth nicht auszuschließen. Negative Auswirkungen wären etwa eine geringere Nutzdatenübertragungsrate.

In der Praxis zeigt sich jedoch, dass bei einem Abstand von mehr als zwei Metern in den meisten Fällen bei keinem der Netzwerke eine wahrnehmbare Verschlechterung der Datenübertragung auftritt. Beträgt die Entfernung zwischen zwei Metern und 50 Zentimetern, ist eine geringfügige Beeinträchtigung erkennbar. Nur wenn die Geräte noch näher beieinander stehen oder direkt nebeneinander positioniert sind, hat dies deutlich wahrnehmbare negative Auswirkungen auf das Funksignal.

Profile und Sicherheit

Unter einem Profil oder Dienst versteht man eine Liste von Optionen oder Funktionen, die für ein bestimmtes Bluetooth-Gerät verfügbar sind. Da die drahtlose Technologie in vielen verschiedenen Anwendungsbereichen eingesetzt wird, muss definiert werden, wie die unterschiedlichen Geräte und ihre Anwendungen zusammenarbeiten sollen. Zu den für ein Bluetooth-Mobiltelefon verfügbaren Profilen oder Diensten können etwa DFÜ-Netzwerk, PIM-(Personal Information Manager-) Synchronisation oder Netzwerkzugriff gehören.

Damit Bluetooth-Geräte zusammenarbeiten können, müssen sie dasselbe Profil besitzen. Wenn Sie ein Headset mit einem Mobiltelefon verbinden möchten, muss also auf beiden Geräten das Profil oder der Dienst „Headset“ vorhanden sein. Möchten Sie auf einem PDA über ein Handy eine DFÜ-Verbindung herstellen, muss auf beiden Geräten das Profil oder der Dienst „Dial-Up Networking“ vorhanden sein. →

PROFI-TIPPS

Wissenswertes zu Bluetooth

Bluetooth und Windows In vielen Fällen lassen sich Probleme, die im laufenden Betrieb auftreten können, durch die Installation des aktuellen Service Packs 2 lösen.

Treiber-Probleme lösen Manche älteren Bluetooth-Treiber vertragen sich nicht mit neuer Software. In diesem Fall müssen Sie die ältere Software deinstallieren, bevor Sie die neuen Treiber einsetzen können.

Wenn ActiveSync streikt Sollte Microsoft ActiveSync über Bluetooth keine Verbindung aufbauen können, kontrollieren Sie zunächst die Aktualität Ihrer Version. Für den Datenaustausch benötigen Sie mindestens ActiveSync 3.5.

Stromverbrauch optimieren Bluetooth ist auf einen äußerst niedrigen Energieverbrauch ausgelegt. Bei den meisten Geräten ist es außerdem möglich, die Bluetooth-Funktion ganz zu deaktivieren, um noch mehr Energie zu sparen oder um die Funk-Funktionen in bestimmten Situationen abzuschalten (zum Beispiel im Flugzeug).

Pairing-Probleme lösen In der Regel läuft das Pairing aller Geräte problemlos ab. Es kann jedoch vorkommen, dass einmal ein Gerät nicht gefunden wird. Sorgen Sie dafür, dass das gesuchte Gerät beim Pairing-Vorgang sichtbar ist. Wählen Sie den entsprechenden Menübefehl oder (bei Geräten mit eingeschränkter Benutzeroberfläche) drücken Sie die zugehörige Tastenfolge. Achten Sie darauf, den richtigen Code oder die richtige PIN einzugeben.

Keine Verbindung? Lässt sich keine Verbindung zwischen zwei Bluetooth-Geräten herstellen, liegt dies normalerweise daran, dass die betreffenden Geräte nicht dasselbe Profil unterstützen. Die Unterstützung eines Profils durch beide Geräte ist jedoch zwingend vorgeschrieben. Sehen Sie im Benutzerhandbuch nach, welche Profile unterstützt werden.

Vorsicht, Lauscher! Bluetooth ist anfällig für heimliche Mitbenutzer: Im Umkreis von zehn Metern können sich Notebook-Besitzer über Ihr Handy ins Internet einwählen. Ganz sicher gehen Sie daher, wenn Sie auf öffentlichen Plätzen die Bluetooth-Funktion abschalten. Das Headset können Sie dann allerdings nicht mehr benutzen.

Bei Bluetooth lassen sich Verbindungsaufbau und Datenübertragung per Verschlüsselung schützen. Sie können diese Sicherheitsoptionen in der Software des Geräts aktivieren. In diesem Fall müssen Sie vor der ersten Verbindung zwischen zwei Geräten – Koppeln oder Pairing genannt – eine maximal 16stellige PIN eingeben. Für spätere Verbindungen mit demselben Partner lässt sich diese PIN speichern. Mit der PIN, einer Zufallszahl und der weltweit einmaligen Geräteadresse bilden die Verbindungspartner einen 128-Bit-Initialisierungsschlüssel. Der schützt den anschließenden Austausch des Verbindungsschlüssels (Link Key). Durch den Link Key, den nur die Geräte kennen, die an einer bestimmten Verbindung teilnehmen, authentifizieren sie sich in einem Challenge-Response-Verfahren.

Auch die übertragenen Daten selbst werden verschlüsselt. Dafür wird aus dem Link Key der Encryption Key berechnet, der acht bis 128 Bit lang sein kann. Zusätzlich verringert das Frequenzsprungverfahren die Gefahr, dass ein Unbefugter mithören kann. Angesichts der sehr begrenzten Reichweite von Bluetooth-Geräten haben Lauscher ohnehin sehr viel geringere Chancen, sich in den Funkverkehr einzuklinken, als bei W-LAN. Dennoch sollten Sie alle vorhandenen Sicherheitsoptionen nutzen und eine ausgefallene, alphanumerische PIN mit maximaler Länge wählen. Zudem können Sie ein Bluetooth-Gerät im Treiber anweisen, nur mit bereits bekannten Gegenstellen Kontakt aufzunehmen. Schließlich lässt sich Bluetooth-Hardware auch vor anderen Bluetooth-Geräten verbergen.

Master und Slaves im Pico-Netz

Die Kommunikation von Bluetooth-Hardware findet innerhalb von Kleinstfunkzellen (Pico-Netzen) statt. In einem solchen Pico-Netz fungiert genau ein Bluetooth-Gerät als Master, das die Kommunikation koordiniert. Alle anderen Teilnehmer in einem Pico-Netz werden als Slaves bezeichnet; sie können nicht direkt miteinander kommunizieren, sondern lediglich mit dem Master-Gerät.

Auswahl von Bluetooth-Geräten
Wählen Sie ein Gerät aus.
Remotegeräte müssen sich im erkennbaren Modus befinden, damit dieser Computer sie finden kann. Informationen dazu, wie ein Remotegerät erkennbar gemacht werden kann, finden Sie in der Dokumentation zum Remotegerät.
NRDICKIE37
Nokia 6600 KK
Nokia 6680hd
Nokia 6600nger
Siemens SX1
Weitersuchen
Alle Geräte anzeigen
Wenn das gesuchte Gerät nicht aufgeführt ist, überprüfen Sie, ob es angeschlossen und betriebsbereit ist. Manche Geräte können nur erkannt werden, wenn eine bestimmte Taste gedrückt wurde.
< Zurück
Weiter >
Abbrechen

PAIRING: Wählen Sie ein Bluetooth-Gerät aus und geben Sie den maximal 16stelligen PIN-Code ein.

In einer Pico-Zelle kommunizieren bis zu acht Geräte miteinander (einschließlich Master). Insgesamt kann ein Pico-Netz jedoch aus maximal 255 Slaves bestehen. Beim Zutritt zu einem Pico-Netz erhält ein Slave eine „Active Member Address“, ohne die keine Datenübertragung an den Master möglich ist.

Bevor eine Verbindung im Pico-Netz aufgebaut wird, befinden sich alle Geräte im „Standby“-Modus. In diesem Modus überwacht das Endgerät passiv alle 1,28 Sekunden den Bluetooth-Frequenzbereich, also den gesamten ISM-Frequenzbereich von 2,402 bis 2,480 GHz. Jedesmal, wenn ein Funkmodul aus dem Schlafmodus aufwacht, kontrolliert es eine Liste von 32 für dieses Gerät definierten Hop-Frequenzen.

Die einzelnen Aktivitätsmodi haben folgende Sendeleistung:

Park Modus: Keine Ausstrahlung, nur Abhören

Hold Modus: Keine Ausstrahlung, nur Abhören (mit MAC-Adresse)

Sniff Modus: Ausstrahlung mit geringer Häufigkeit, abhängig von der Anwendung (Pausenzeiten zwischen 0,6 Millisekunden und 40,9 Sekunden)

Geht ein Slave auf eigene Anforderung oder auf Anweisung des Masters in den Park-Modus über, wird ihm die „Active Member Address“ entzogen und er erhält eine „Parked Member Address“. Wenn tatsächlich 255 Slaves in einem Pico-Netz angemeldet sind, müssen sich mindestens 248 von ihnen im Park-Modus befinden, da ja nur maximal acht Geräte in einer Pico-Zelle kommunizieren können. Ein Pico-Netz definiert sich ausschließlich über die am Master angemeldeten Slaves. Dank Frequenz-Hopping können bis zu zehn Pico-Netze in physikalisch überlappenden Funknetzen koexistieren. Ein Bluetooth-Gerät kann Mitglied in mehreren Pico-Netzen sein, die sich wiederum zu so genannten Scatter-Netzen zusammenschließen lassen.

So funktioniert das Pairing

Das Pairing dient der Überprüfung der Zutrittsberechtigung eines Bluetooth-Gerätes zu einem Pico-Netz. Im Verlauf dieser

KNOW-HOW

PANs, MANs und WANs

Computer-Netzwerke unterteilt man anhand ihrer räumlichen Ausdehnung und ihres Einsatzbereichs in verschiedene Kategorien. Abgesehen vom bekannten Local Area Network (LAN), dem privaten oder professionellen Kabelnetz mit einer Ausdehnung von zehn bis mehrere hundert Meter sind das die fogenden Netzwerke:

PAN (Personal Area Network): Damit ist die Vernetzung von PCs, PDAs und Mobiltelefonen im Wohnumfeld gemeint. Die Vernetzung kann über Kabel (USB, Firewire) oder drahtlos mit Bluetooth, W-LAN oder Infrarot erfolgen. Die Ausdehnung beträgt zehn bis 30 Meter.

MAN (Metropolitan Area Network): Ein MAN ist ein breitbandiges, in Glasfasertechnologie aufgebautes Telekommunikationsnetz, das überwiegend eine ringförmige Struktur aufweist und die wichtigsten Bürozentren einer Großstadt miteinander verbindet. Ein Metropolitan Area Network kann eine Ausdehnung von bis zu 100 Kilometern haben.

WAN (Wide Area Network): Beim WAN handelt es sich um ein großräumiges Netzwerk, das mehrere LANs über weite Strecken verbindet. Ein Beispiel für ein WAN wäre ein Netzwerk, das mehrere Filialen einer Firma in einem Land verbindet.

DER EXPERTEN-TIPP

Noch komfortabler mit Daten hantieren

Daten blitzschnell übertragen Nach einem Geschäftstermin ist das Notebook gespickt voll mit wichtigen Daten. Die Wartezeit am Flughafen ist die optimale Gelegenheit, die Daten auf den PDA zu überspielen – kein Problem mit den Bluetooth-USB-Adaptern von Belkin. Damit kann der Reisende seine Daten kabellos und in einem Radius von bis zu 100 Metern an bis zu sieben weitere Bluetooth-fähige Geräte übertragen.

Drucken via Bluetooth Das Notebook muss griffbereit sein, aber der Nutzer möchte keine Anschlusskabel mit sich herumschleppen – auch nicht, wenn er Dokumente drucken will. Mit dem Bluetooth-USB-Druckeradapter von Belkin, der einfach am Drucker angesteckt wird, muss man nicht erst die Daten von mobilen Geräten auf den PC kopieren oder sich mit dem Ethernet verbinden, um sie zu drucken. Das Aufbauen von Kabelverbindungen gehört dank der Bluetooth-Technologie der Vergangenheit an. Auch unterwegs ist der USB-Druckeradapter ein nützlicher Begleiter, da er sich mit jedem USB-Drucker verbinden lässt.

Freisprechen mit Bluetooth Beim Autofahren kann das Kabel der Freisprecheinrichtung richtig nerven. Um lästige Kabel loszuwerden und trotzdem das Hantieren mit dem Handy zu vermeiden, ist die federleichte Bluetooth-Freisprecheinrichtung von Belkin eine gute Wahl. Gespräche lassen sich mit einem Tastendruck am Ohrhörer annehmen oder auslösen, sodass der Fahrer nicht zum Handy greifen muss.

CHIP EXPERTE

Stefan Bönsch (38) ist Regional Director Central Europe bei der Belkin Components GmbH und für die Leitung der Geschäfte der deutschen Niederlassung in München zuständig. Belkin Components ist einer der weltweit führenden Hersteller von Peripheriegeräten und Connectivity-Lösungen für Nutzer von Computern und Consumer Electronics. Heute beschäftigt das US-Unternehmen rund 1.400 Mitarbeiter in Büros in Nordamerika, Europa und Australien.

→ www.belkin.com/de

Prozedur wird ein Verbindungsschlüssel mit 128 Bit Länge erzeugt und für alle künftigen Verbindungen in den beiden Geräten gespeichert. Zur gesicherten Übertragung dieser Zufallszahlen muss zuvor ein Initialisierungsschlüssel angelegt worden sein. Das Pairing findet ausschließlich beim ersten Kontakt zweier Bluetooth-Geräte statt. Ist das einmal geschehen, wird das Bluetooth-Kennwort bei erneuter Prüfung der Zutrittsberechtigung nicht mehr benötigt. Bei jeder weiteren Prüfung wird stattdessen der Verbindungsschlüssel verwendet.

Der Verbindungsschlüssel dient ausschließlich der verschlüsselten Prüfung der Zugangsberechtigung. Auf seiner Basis wird allerdings ein weiterer Schlüssel mit einer Länge zwischen acht und 128 Bit angelegt. Dieser Schlüssel dient der Absicherung der Datenübermittlung und wird für jede Sitzung neu ausgehandelt. Die maximale Länge dieses Sicherungsschlüssels hängt von der verwendeten Hardware ab.

Trotz der standardisierten Profile ist es nicht immer ganz einfach, zwei Bluetooth-Geräte zu verbinden. Je nachdem, ob es sich dabei etwa um USB-Adapter, Headset, Handy oder PDA handelt, fallen die Schritte unterschiedlich aus, folgen aber immer diesem Muster:

1. Installation Schließen Sie das Bluetooth-Gerät an und installieren Sie Treiber und Steuerungs-Software von der mitgelieferten CD. Ältere Windows-Versionen unterstützen Bluetooth nicht, deshalb benötigen Sie den Hersteller-Treiber. Windows XP findet Bluetooth-Geräte dagegen automatisch. Dort können Sie es anschließend mit Hilfe der Systemsteuerungsoption „Bluetooth-Geräte“ installieren.

2. Gerätesuche Öffnen Sie unter Windows XP in der Systemsteuerung das Applet „Bluetooth-Geräte“. Aktivieren Sie dann auf der Registerkarte „Optionen“ das Kontrollkästchen „Suche aktivieren“, damit andere Bluetooth-Geräte Ihren Computer finden. Anschließend aktivieren Sie die Kontrollkästchen „Bluetooth-Geräte können eine Verbindung mit diesem Computer herstellen“ und „Benachrichtigung anzeigen, wenn ein Bluetooth-Gerät eine Verbindung herstellen möchte“.

3. Dienste auswählen Öffnen Sie in der Systemsteuerung das Applet „Bluetooth-Geräte“. Klicken Sie auf der Registerkarte „Geräte“ auf die Hardware, für die Sie Dienste aktivieren möchten, und klicken Sie auf „Eigenschaften“. Wählen Sie anschließend auf der Registerkarte „Dienste“ die gewünschten Dienste aus.

4. Geräte verbinden Öffnen Sie in der Systemsteuerung das Applet „Netzwerkverbindungen“. Klicken Sie unter „PAN (Personal Area Network)“ auf das Symbol „Bluetooth-Netzwerkverbindung“ und lassen Sie sich unter „Netzwerkaufgaben“ die „Bluetooth-Netzwerkgeräte anzeigen“. Klicken Sie anschließend auf die Hardware, mit der eine Verbindung hergestellt werden soll, und wählen Sie dann die Option „Verbinden“.

Falls keine Verbindung zustandekommt, kann das daran liegen, dass das Bluetooth-Gerät ausgeschaltet, außer Reichweite oder nicht für eingehende Verbindungen konfiguriert ist. Überprüfen Sie das Gerät und versuchen Sie erneut, die Verbindung via Bluetooth herzustellen.

Peter Klau

KNOW-HOW

Die drei Sendeleistungsklassen von Bluetooth

Klasse	Sendeleistung in Watt	Sendeleistung in dBm	Reichweite
Klasse 3 Leistungsregelung optional	bis 1 mW	bis 0 dBm	10 Meter freies Feld, 5 bis 7 Meter im Büro
Klasse 2 Leistungsregelung optional	0,25 bis 2,5 mW	-6 dBm bis 4 dBm	30 Meter
Klasse 1 mit Leistungsregelung von 2,5 mW bis 100 mW	1 bis 100 mW	0 dBm bis 20 dBm	100 Meter (Long-Range Bluetooth)

Was Blackberry leistet

Immer per Mail erreichbar

E-Mails sofort nach ihrem Eintreffen im Firmennetz auf dem Handheld lesen – Blackberry macht's möglich. Was bisher ausschließlich Managern vorbehalten war, wird nun auch für Privatnutzer interessant: T-Mobile, Vodafone und O2 bieten bereits passende Tarife an. Wie Blackberry funktioniert, zeigt Ihnen dieser Beitrag.

Die TV-Werbung von T-Mobile in den letzten Wochen machte es offensichtlich: Blackberry wird populär. Die drahtlose Kommunikationslösung besteht aus Handheld-Geräten, Rechenzentren sowie Software und Diensten. Die Technik hinter Blackberry leitet Kopien von Nachrichten, die etwa in der Firmen-Mailbox eingehen, an ein mobiles Endgerät weiter – ähnlich wie ein Exchange Server im Unternehmen, der E-Mails in die Inbox eines Arbeitsplatzrechners schiebt.

Der ursprüngliche Zweck von Blackberry war es, Power-Usern das lästige Abrufen von E-Mails per Handy und Notebook zu ersparen. Research In Motion (RIM), Entwickler und Lizenzgeber der Blackberry-Technik aus Waterloo in Kanada, sorgt mit seiner Erfindung bisher besonders im Markt der Unternehmenskommunikation für neuen Schwung.

Ständig mit der Zentrale verbunden

Die Handhelds sind per Mobilfunk permanent mit der Firmenzentrale verbunden. Sie nutzen dazu eine „Always-on"-Funktionalität, die in Europa über die paketbasierende Funktechnik GSM/GPRS realisiert wird. Zum Aufrechterhalten der Verbindung müssen nur kleine Datenmengen mit geringer Leistung gesendet werden, daher erreichen die Endgeräte lange Laufzeiten von bis zu fünf Tagen.

Research in Motion hat die Systemfunktionalität inzwischen erheblich erweitert: Mittlerweile kann man mit den Geräten telefonieren, SMS/MMS versenden und im Internet surfen. Die Anbindung an CRM- (Customer Relationship Management-), ERP- (Enterprise Ressource Planning-) und Dokumenten-Management-Anwendungen ist ebenfalls möglich. Da Blackberry als offenes System entwickelt wurde, lässt es sich durch eigene Java-Programme erweitern.

Dreistufige Datenübertragung

Die Datenübertragung innerhalb der Blackberry-Architektur verläuft in drei Phasen: Aufbereitung der Kommunikationsdaten im Unternehmen, Übertragung via Internet zum Mobile Routing Center und schließlich Weiterleitung über den Mobilfunkanbieter, bei dem das Endgerät eingebucht ist, an das Blackberry-Handheld (siehe Grafik auf der nächsten Seite). Wichtig dabei: Die gesamte Übertragung vom Unternehmen bis zum Endgerät (und zurück) erfolgt verschlüsselt. RIM vertraut auf das als sicher geltende Encryption-Verfahren Triple-DES (Data Encryption Standard) mit einer Schlüssellänge von 168 Bit oder – ab der gerade eingeführten Blackberry-Version 4 – auf das noch stärkere AES-Verfahren (Advanced Encryption Standard).

Externe Schaltzentrale

Dreh- und Angelpunkt in diesem System sind die Mobile Routing Center: Diese mehrfach redundant aufgebauten Rechenzentren bilden die Schnittstelle zwischen den Unternehmen, die Blackberry einsetzen, und den Mobilfunkanbietern, die die Verbindung zum Endgerät herstellen. Weltweit sind derzeit drei dieser Mobile Routing Center im Einsatz, sie versorgen die Großräume Amerika, Asien/Pazifik sowie Europa. Das für Europa zuständige Center befindet sich in der Nähe von London. Es unterhält direkte Verbindungen zu allen bedeutenden Mobilfunkanbietern und Internet Service Providern (ISP). Diese Routing Center schotten die Endgeräte über eine mehrstufige Sicherheitsarchitektur vollständig vom öffentlichen Internet ab. Da die IP-Adressen der Handhelds von außen nicht sichtbar sind, ist ein direktes Hacken so gut wie unmöglich.

Blackberry mit proprietärem Protokoll

Nach dem Einschalten sucht das Blackberry-Handheld das nächste verfügbare GSM-Netz und bucht sich ein. Danach fordert es eine paketbasierende GPRS-Verbindung an. Es bekommt eine IP-Adresse zugewiesen und meldet sich damit und mit seiner geräteeigenen Identifikationsnummer beim Mobile Routing Server an. Liegen dort aktualisierte PIM-Daten (Personal Information Management) vor, werden sie sofort mit dem Java-basierenden Blackberry-Client auf dem Handheld abgeglichen.

Die Endgeräte halten zwar über die Mobilfunkbetreiber die Verbindung zum Routing Center, ihre Datenströme werden jedoch nie direkt weitergeroutet. Gleiches gilt für die umgekehrte Richtung: Daten vom Unternehmen erreichen über den Service Provider und das Internet zwar das Routing Center, aber nicht direkt das Endgerät. Das Routing Center fungiert quasi als Übersetzer und Verladestation: Es verteilt den vom Unternehmen kommenden und auf dem Internet-Protokoll (IP) basierenden Datenstrom auf einen Übertragungsmechanismus, der mit einem von RIM entwickelten, proprietären Protokoll-Stack arbeitet. Neben der Sicherheit stand bei dessen Entwicklung

CHIP → DVD-CODE Blackberry

→ **Software-Sammlung** Auf der Heft-DVD finden Sie eine Zusammenstellung von genialen Blackberry-Tools, die Ihnen die Arbeit mit Ihrem Gerät erleichtern. In der Sammlung finden Sie zum Beispiel die mobile Office-Suite eOffice für bequemes Arbeiten unterwegs, die Fax-Lösung Mail2fax oder den Chat-Client VeriChat for Blackberry.

Die besten Blackberry-Tipps im Web

Deutsche Homepage → www.blackberry.com/de
Aktuelle Infos zu Geräte, Software, Anwendungen, Technik
Blackberry-Support
→ www.blackberry.com/knowledgecenter Technische Informationen, Fehlerbehebung und Tipps in englischer Sprache
Tipps & Tricks → www.joern.de/BB
Jede Menge Blackberry-Tipps und -Anleitungen sowie zahlreiche weiterführende, nützliche Links

die Übertragungsgeschwindigkeit im Fokus. So basiert der Protokoll-Stack zwar auf der verbreiteten Kombination TCP/IP, verzichtet unter anderem aber auf die darin implementierten Fehlertoleranz-Mechanismen. Die sind bei einer leitungsgebundenen Übertragung sinnvoll, bremsen jedoch die Kommunikation auf Funkstrecken stark aus.

Der Gegenpart für die Mobile Routing Center ist der so genannte Enterprise Server. Die komplexe, modular aufgebaute Software ist hinter der Firewall eines Unternehmens installiert. Sie bildet die Schnittstelle zwischen der externen Internet-Infrastruktur und der im Unternehmen verwendeten Kommunikations-Software, beispielsweise Microsoft Exchange, IBM Lotus Domino oder Groupwise. Von dort aus kann der Enterprise Server auf Firmendaten zugreifen, die auf den Mail-, Applikations- und Web-Servern liegen.

Mobile Data Service leitet E-Mails weiter

Eine Hauptkomponente des Enterprise Servers ist der „Mobile Data Service“: Darin ist die eigentliche „Push“-Funktionalität implementiert, über die etwa Kopien eingehender E-Mails an das mobile Endgerät gesendet werden. Kommen in großen Unternehmen mehrere Enterprise Server zum Einsatz, lässt sich ein Mobile Data Service als Master konfigurieren, der den „Push“-Dienst für alle Endgeräte übernimmt.

RIM verwendet für die Verschlüsselung die als sicher geltenden symmetrischen Verfahren Triple-DES oder AES. Nach Einschätzung von „@stake“, eines Beratungsunternehmens für digitale Sicherheit, bietet „das Blackberry-Security-Modell damit das gleiche Maß an Sicherheit wie eine herkömmliche VPN-Verbindung“. Mit einem virtuellen privaten Netzwerk (VPN) lässt sich die Funktionsweise von Blackberry tatsächlich gut vergleichen – mit dem Unterschied, dass die RIM-Technik den Anwendern die oftmals komplizierte Einrichtung des VPN-Tunnels erspart.

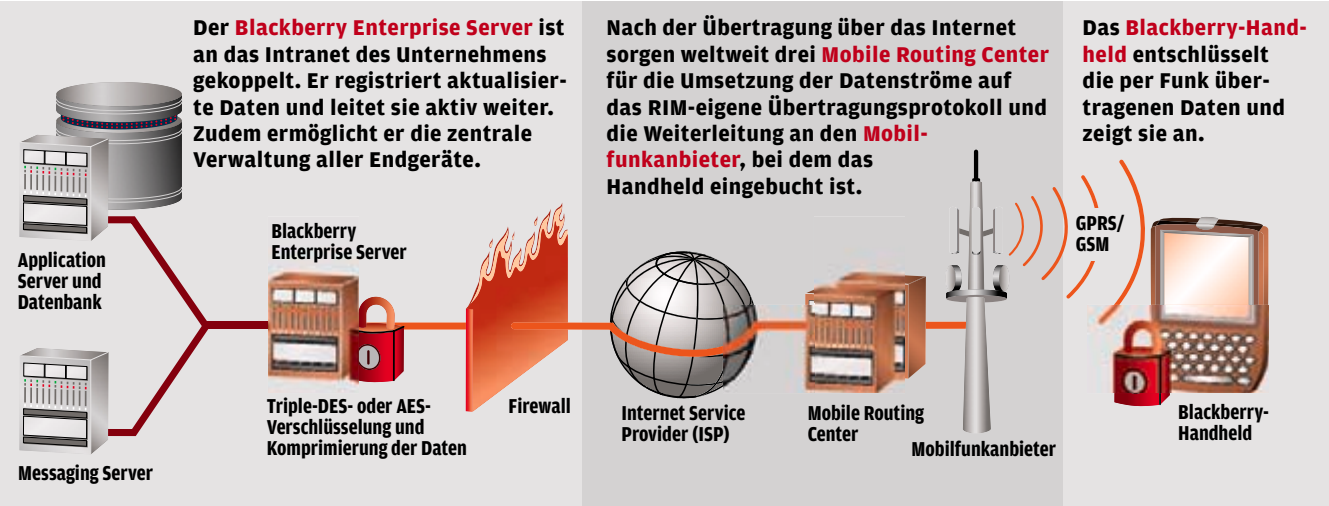
Um die verfügbare, auf Funkübertragungsstrecken nach wie vor verhältnismäßig geringe Bandbreite bestmöglich zu nutzen, verschlüsselt der Enterprise Server die ausgehenden Daten nicht nur, er komprimiert sie auch. Außerdem sorgt er dafür, dass nach Möglichkeit nur die Daten übertragen werden, die der Anwender gerade auf seinem Handheld betrachtet. Scrollt der Nutzer etwa in einer E-Mail zur nächsten Display-Seite, schiebt der Enterprise Server genau die für die Anzeige benötigte Datenmenge auf das Endgerät. In der Regel sind diese „Häppchen“ lediglich 1 bis 2 KByte klein und landen entsprechend schnell beim Empfänger. Blackberry ist also so gesehen eine Art E-Mail-Fernbetrachtungsmaschine. Wichtige Daten lassen sich jedoch auf dem Handheld auch speichern – so sind sie auch dann einsehbar, wenn einmal kein Mobilfunknetz verfügbar sein sollte. Der gleiche Mechanismus kommt für das Betrachten anderer Daten zum Einsatz, beispielsweise Bilder, Word- oder PDF-Anhänge.

In abgespeckter Form bieten T-Mobile sowie Vodafone den E-Mail-Pushdienst mitsamt den Blackberry-Endgeräten auch für Privatkunden an. Dabei kommen vorkonfigurierte Handhelds zum Einsatz. Je nach Anbieter fallen monatliche Gebühren von ungefähr 20 Euro an. Diese Lösungen sind jedoch nicht mit der ausgewachsenen – und teureren – Unternehmenslösung vergleichbar, sondern eher mit einem komfortablen Handy-E-Mail-Client.

Michael Eckstein

KNOW-HOW

So überträgt Blackberry Daten vom Unternehmen zum Endgerät


Der Blackberry Enterprise Server ist an das Intranet des Unternehmens gekoppelt. Er registriert aktualisierte Daten und leitet sie aktiv weiter. Zudem ermöglicht er die zentrale Verwaltung aller Endgeräte.
Nach der Übertragung über das Internet sorgen weltweit drei Mobile Routing Center für die Umsetzung der Datenströme auf das RIM-eigene Übertragungsprotokoll und die Weiterleitung an den Mobilfunkanbieter, bei dem das Handheld eingebucht ist.
Das Blackberry-Handheld entschlüsselt die per Funk übertragenen Daten und zeigt sie an.
Application Server und Datenbank
Messaging Server
Blackberry Enterprise Server
Triple-DES- oder AES-Verschlüsselung und Komprimierung der Daten
Firewall
Internet Service Provider (ISP)
Mobile Routing Center
Mobilfunkanbieter
GPRS/ GSM
Blackberry-Handheld

Info-Grafik: H. Fuchsloch

Alle Programme auf DVD

Vollversionen

Intranator Enterprise-Edition → 36
Der Linux-basierte Security-Server bietet allen Usern im Netz Webzugang, Mailserver, Firewall und integrierten Virenschutz

Back Protection 2004
Das Tool schützt wichtige und vertrauliche Daten vor unbefugtem Zugriff über lokale Netzwerke, Internet oder Spyware

Ace Backup 2003 → 36
Die Backup-Software sichert Ihre wichtigsten Dateien vollautomatisch oder manuell bequem mit Hilfe von Assistenten

W-LAN

Aerosol 0.65 78
aircrack 2.1
Airfart 0.21
AirJack 0.6.6b-alpha
AirMagnet Laptop Analyzer 4.0 99
AiroPeek SE 2.05 125
Airscanner Mobile Antivirus Pro
Airscanner Mobile Encrypter
Airscanner Mobile Firewall
AirSnare 0.67 77
AirSnort 0.2.7e 54
AirTraf 1.1 125
AP Hopper 0.3alpha
AP Radar 0.52
Aphunter
APSniff 0.2
APTools 0.1.0
Asleap 1.4
Auditor security collection 081004-01
BSD-AirTools 0.2
BSI-Broschüre „Sicherheit im Funk-LAN“ 1.1
Cqure AP 2.5.0
DMZS-Carte
FakeAP 0.3.1 125
Hotspotter 0.4
iStumbler 90 125
KisMAC 0.12a 125
Kismet 2005-01-R1 125
libpcap 0.8.3
LinkFerret Network Monitor 3.10
Local Area Security Linux 0.5
MacStumbler 0.75b 125
MiniStumbler 0.4.0 125
Mognet 1.16 125
NetChaser 1.51
Network Stumbler 0.4 78
NoCatAuth 0.82
Packetyzer 3.03
PHLAK 0.2-1
PocketWarrior 29052003
Pong 1.1
PrismStumbler 0.7.3
Snort-Wireless 2.01. Alpha 03
SSIDsniff 0.36 125
Tcpdump 3.8.3
THC-LEAPcracker 0.1
urld für Linux 2
urld für Windows 2
void11 0.2.0
WarGlue 1.0
WarLinux 0.5
Wavelan Tools 0.1
WaveMon 0.4.0b für
WaveStumbler 1.2.0
WellenReiter 1.9 125
WepAttack 0.13
WEPCrack 0.10 125
Weplab 0.1.3
WEPWedgie 0.1.0-alpha
Wi-Find 0.2.1
WiFiFoFum 0.3.3
WifiScanner 0.9.5
WifiStatd 0.1a
WinDump 3.8.3 beta
WinPcap 3.0
Wireless Access Point Utilities for Unix 1.4.1 125
WiStumbler 1.3
WLAN Expert 1.0
wscan 2.0

ADMINISTRATION

602LAN Suite 2004.0.04.0913
Absolut Time Corrector 3.6
Absolut Time Server 2.2
AdmWin 6.05
Advanced Remote Info 0.6.3.8
Aegis Client für 2000/XP 2.2
Aegis Client für CE.Net 2.1
Aegis Client für Linux 2.1x
Aegis Client für PocketPC 2.1
Apache HTTP-Server Linux 2.0.52
Apache HTTP-Server Windows 2.0.52
Bemused 1.73
Comparator 2.2
Domain Administration Tool 3.20
EasyChat 3.00 RC5
Ethereal 0.10.9 123
Ethereal Linux 0.10.9
EventSentry Light 2.41a
FB Joker 2.9.1.0
IA eMailServer Corporate 5.3.2
IA eMailServer Standard 5.3.2
Ideal Administration 5.41
Intellipool Network Monitor 2.3
JAB 3.0
JanaServer 2.4.5.1
LAN Shut-Down 1.0
LanFlow 4.19 für
LANMailServer 1.02
Look@LAN 2.50 build 29 123
Magic NetTrace 2.5.5
MDaemon Mailserver 7.2.2
MultiNetwork Manager 7.01.0018 144
MySQL 4.1.9
MySQL 4.1.9
Netcat 1.1
NetCommy 1.14
NetConnect 1.01
NetIO 1.23
NetSender Pro 2.60
NetSetMan 1.10 123
Netswitcher 3.2.6
nmap 3.75
NmapWin 1.3.1 123
Paessler Router Traffic Grapher 4.1
Parents Friend Light-Version 6.0
PHP SysInfo 2.3
PIKT 1.18.0b
Postman 1.6
PPPshar Accelerator
PPPshar Pro 1.9
Public ShareFolder 1.2
Public SyncTool 1.1
PuTTY 0.56
Qualimail SMTP Server 1.0 build 4357
Remote Administrator 2.2
Service Pack Manager 2000 6.9.9.3
Service Pack Manager 2000 5 User 6.9.9.3
The Personal FTP Server 4.46
The Personal FTP Server Pro 4.9
TimeServer 1.82
Tunnelier 3.60a
VNC für Linux 4.0
VNC für WIN 4.0
War FTP Daemon 1.70 Beta 1
Winfingerprint 0.6.0
WinGate 5.2.2
WinInterrogate 0.1.7
WinPcap 3.0
WinProxy 5.2
WinSSHD 3.30a

BLACKBERRY

ChronoMagic 1.0.2
CryptMagic 2.0.1
Dream Meanings Dictionary 2.5
EmailViewer Personal Edition 3.5
English Language Acronyms Dictionary 2.5
eOffice Professional Edition 2.1
eZcase 1.1
GotMailViewer 3.0
HotViewer 3.0
Mail2Fax 1.2.1
ShopMagic 1.0.2
TimeMagic 1.2
VeriChat for Blackberry 1.78b
WebViewer 4.0
WorldMagic 1.2.3

SECURITY

0190 Alarm 3.70
0190 Warner 4.03
AceBackup 2.1
Ad-aware SE Personal 1.0.5
Alle meine Passworte (AmP) 2.21
AntiVir Personal Edition 6.29.00.03
avast! 4 Home 4.5.561
AVG Anti-Virus Free 7.0 Build 300
a² free 1.5.2
BackUp Maker 3.2
BitDefender Free 7.2
Claviscom SCHREDDER 5.2
ClearProg 1.4.1
CompuSec PC Security Suite 4.17
CryptoSoft Enigma 1.4
CWShredder 2.12
Dialer Control 1.3.2
Eraser 5.7
ERUNT 1.1g
F-Prot für DOS 3.16a
Global Safe Disk 1.93.1
HijackThis 1.99
IMsecure free 1.0.2.0
JAP 00.02.004
Kerio Personal Firewall 4.1.2
Knocker 0.66
MobileAssistant 1.6
Outlook Express BackupTool 2.1
Outpost Firewall 1.0.1817
Password Depot 1.7
PINs 4.50
POPFile 0.22
PopUpKiller & DialerDetector 2.2.5
secretmaker 3.9.8
SecuLock! 1.0
Secure 4 U Lite 5.0
Secure Eraser 1.1
Spamihilator 0.9.8.4
SpamPal 1.591
SpyBot-Search & Destroy 1.3
Stunnel 4.05
SuperSpamKiller 2.00
Sygate Personal Firewall 5.6
Sygate Personal Firewall Pro 5.5
TrojanHunter 4.1
WinPatrol 7.0.1.0
WinSCP 3.7.1
XPAntiSpy 3.93
ZoneAlarm 5.5.062 77

SYSTEM

7-Zip 3.13
AIDA32 3.93
ATITool 0.0.23
Bart's PE Builder 3.1.3
BBIE - Bart's Boot Image

Software und andere auf dieser DVD gespeicherten Werke werden unter Ausschluss jeglicher Gewährleistung und ausschließlich zum privaten Gebrauch überlassen. Die Haftung für mittelbare Schäden oder entgangenen Gewinn ist ausgeschlossen. Produktbezeichnungen u. Logos sind Eigentum d. jeweiligen Inhaber als Warenzeichen und eingetragene Warenzeichen geschützt. © Copyright 2005 Vogel Burda Communications GmbH.
CHIP PROFESSIONELL
VOLLVERSIONEN
02|05
INTRANATOR
Zentraler Security-Server auf Linux-Basis, stellt Netzrechnern Internet-Zugang, Firewall, Mail-und Fax-Server zur Verfügung, schützt Clients durch AntiVirus-Gateway, sichere Verbindung dank Proxy-Server und VPN-Unterstützung
BACK PROTECTION 2004
Wichtige Dokumente und Dateien vor unbefugtem Zugriff über lokale Netze, Internet oder Spionage-Tools schützen, Kommunikationsverschlüsselung, vertrauliche Daten sicher vernichten
ACE BACKUP 2003
Wichtige Daten zeitgesteuert und manuell sichern lassen, starke Komprimierung, unknackbare Verschlüsselung
Die DVD enthält keine jugendbeeinträchtigenden Inhalte.
WIRELESS-TOOLKIT
SNIFFER-TOOLS
Network Stumbler 0.4.0, Kismet 2005-01-R1, iStumbler 90, MiniStumbler 0.4.0, WiFiFoFum 0.3.3, PocketWarrior 29052003, Wellenreiter 1.9, AirMagnet Laptop Analyzer 4.0, KisMAC 0.12a
W-LAN-KEYTESTER
aircrack 2.1, AirSnort 0.2.7e, Asleap 1.4, Pong 1.1, THC-LEAPcracker 0.1, WepAttack 0.1.3, WEPCrack 0.1.0, weplap 0.1.3, WEPWedgie 0.1.0-alpha
WIRELESS-SECURITY
Aegis Client 2.2, 602LAN Suite 2004.0.04.0913, Intellipool Network Monitor 2.3, Winfingerprint 0.6.0, Service Pack Manager 2000 6.9.9.3, nmap 3.75
FIREWALL + ANTIVIRUS
Sygate Personal Firewall 5.6, Outpost Firewall 1.0.1817 Kerio Personal Firewall 4.1.2, Zone Alarm 5.5.062, avast! 4 Home Edition 4.5.561, AntiVir PE, AVG Anti-Virus Free 7.0 Build 300
BLACKBERRY-TOOLS
CryptMagic 2.0.1, VeriChat f. Blackberry 1.48b eOffice Professional Edition 2.1 WebViewer 4.0, Mail2Fax 1.2.1
u.v.m.
Bei den Programmen handelt es sich um Free- oder Shareware.

Extractor 1.0
CDmage 1.01.5
Dr. Hardware 2005 v6.0
Filemon 6.12
FreeMem Professional 5.2
Fresh Diagnose 6.90
FreshUI 7.26
GetDataBack for FAT 2.31
GetDataBack for NTFS 2.31
Hardcopy 15.1
HDCleaner 2.360
Hotkeycontrol XP 4.2.1
Joe 3.3
Microsoft Baseline Security Analyzer 1.2.1
Motherboard Monitor 5.3.7.0
Nero CD-DVD Speed 3.61
nLite 0.99.7
Notepad2 1.0.12
PC Inspector File Recovery 3.0
PDFCreator 0.8.0
Powertweak 0.99.4
RAM Idle LE 1.4.7.2
RegCleaner 4.3.0.780
RegCool 3.011
Registry Optimierer 2.0.1
Registry System Wizard 1.5.9
Registry Toolkit 3.5
Regmon 6.12
RegSeeker 1.35
ResBuilder 2.10
SiSoft Sandra Lite 2005
Tweak Master 2.04 Build 764
TweakOE 2.1
TweakPower 1.045
TweakUI 2.10
WINner Tweak SE 2.8.1
Wintuning Kit Standard
X-Setup Pro 6.6 Final
ZipGenius Suite 5.5.1
ZipStar 4.2

| INTERNET |

ADSLKeepAlive 3.2
Amicron Mailoffice 2.0
AutoDialUp 3.6.2.1
Avant Browser 10.0 Final
Bookmark-Manager 3.0.1
Casc'ADSL 0.99
cFosSpeed 1.0.8
DFÜ-Speed 2.2
Download Accelerator Plus 7.4
DownloadSpeed 1.3.1
DSLWatch.NET 1.4
DU Meter 3.07 Build 192
DUN-Backup 1.02
Eudora 6.2
FlashGet 1.65
flat2serv SoftRoute 1.6
FoxMail 5.0.8
Gaim 1.1.1
GeMail 2.6
Go!Zilla 4.11.39
Googlefilter 2.0
GPU Windows 0.9081
Gravity 2.7
ICQ Lite 4.1.1718
IncrediMail Xe #1787
LAN-eMail 2004.12.1092
LAN-eMail Pro 2004.12.1133
LeechGet 2004 1.1
Meine Traffic 2.0
Miranda IM 0.3.4a
Mozilla 1.7.5
Mozilla Firefox 1.0 Final
Mozilla Sunbird 0.2 RC2
Mozilla Thunderbird 1.0
MSN Messenger 7.0 Beta
NetMail Light 4.27
Netscape Complete 7.10
Odigo 4.0 Build 689
OnlineEye 2.11
OnlineEye Professional v1.4.9c
OnlineMonitor 3.10
OnlineOptimizer 2.05
OnlineTimer Pro 11.11
Opera 7.54 (Java Version)
Pegasus Mail 4.21c
Ping Plotter 1.10
Redialer 1.30.0.7* Final
RouterControl 1.4
Schmaili 5.1
Simple Instant Messenger 0.9.3
Skype 1.1.0.73
SlimBrowser 4.03
SmartFTP 1.0 Build 983
StarDownloader 1.43
Trillian 3.0 Basic
WinHTTrack 3.32.2
WinTracert 2004.8.18
WT-Rate 3.60

| BASICS |

Access 97 Snapshot Viewer
Audacity 1.2.3
Audiograbber 1.83
BSPlayer 1.0.2
Burn4Free 1.0.6.0
Burrrn 1.12
CDBurnerXP Pro 3.0.116
CDex 1.51
ClipInc 1.50a
CoolPlayer Build 215
CUEcards 2.21
DeepBurner 1.3.6
DiaShow XP 4.5
DirectX 9.0c
DivX Standard
DVD Genie 4.10
Excel Viewer 2003 v1.0
FreeRip 2.92
GIMP 2.2.1
GIMP für Linux 2.2.1
GoldWave 5.08
GSpot 2.52 Beta 1
GTK+ for Windows 2.4.14
GX::Transcoder 2.1
iRaTe 2 v2003.1.0.9
IrfanView 3.95
ISO Recorder 2.0 Beta 2
IsoBuster 1.7
jetAudio 6.0.6 Basic
K!TV XP 1.2.6.0
LAME 3.96
Mainhatten Office 5.3.4
nexTView EPG 2.7.4
On2Share 1.0.0.10
onlineTV 2.0.0.5
OpenOffice 1.1.4
OpenOffice
PhotoFiltre 6.0.2
PowerPoint 2003 Viewer 3.0
ProgDVB 4.47
QCD Player 4.51
RawWrite
RealPlayer 10.5 Gold
Sceneo Vcopy 1.28
TV-Browser 1.0 Final
TVgenial 3.30
VideoInspector 1.2.2
VideoLAN Client 0.8.1 140
Vidomi 0.469
Vidomi Patch
VirtualDub 1.6.3 Exp.
WinAmp Full 5.0.8c 90
Windows Media Player 10.0
WinTer 4.2.02
Word Viewer 2003 v1.0
WordToPDF 1.9
Xenorate 2.20
Zoom Player Standard 4.10 Beta 2

CHIP W-LAN-Toolbox

Die besten Wireless-Tools

Auf der Heft-DVD finden Sie die besten Free- und Shareware-Tools rund um „Wireless Networking“ in den jeweils aktuellsten Versionen. Drei Vollversionen – ein kompletter Server, ein Wireless-Tuning-Tool und eine Backup-Lösung – runden das Paket ab. Mit dieser Sammlung sind Sie für alle Aufgaben im W-LAN-Betrieb vorbereitet.

Planen, optimieren und testen – die CHIP-Professionell-Heft-DVD bietet Ihnen die passenden Tools, um Ihr drahtloses Netz so sicher wie möglich zu machen. Über 350 Free- und Shareware-Programme, zum Beispiel W-LAN-Sniffer, Portscanner, Administrations- und Fernwartungs-Tools sowie Intrusion-Detection-Systeme zum Schutz vor Hackern, erleichtern Ihnen die Arbeit als Admin eines Wireless LAN.

Drei Top-Vollversionen für W-LAN-Profis

Zusätzlich zur besten Free- und Shareware finden Sie drei Vollversionen auf der Heft-DVD, die sich hervorragend zu einem kompletten Sicherheitspaket ergänzen.

Die **Intranator Enterprise-Edition** von Intra2net ist ein professioneller Security-Gateway auf Linux-Basis, über den alle Rechner in Ihrem Netzwerk auf das Internet oder E-Mails zugreifen. Der integrierte E-Mail-Server stellt jedem Anwender ein E-Mail-Konto mit Viren- und Spam-Schutz zur Verfügung. Über einen Proxy-Server legen Sie fest, welche Inhalte Ihre Benutzer im Web sehen dürfen. Die Verwendung von Virtuellen Privaten Netzen (VPN) sowie Firewall und Virenschutz garantieren sichere Verbindungen zwischen LAN und Internet.

Mit **Back Protection 2004** erhalten Sie eine Komplett-Lösung zum Schutz wichtiger und vertraulicher Daten vor unbefugtem Zugriff. Die Software schützt Ihre Dokumente im Hintergrund vor Angriffen über lokale Netze, das Internet oder durch Spionage-Software. Auf Wunsch verschlüsselt Back Protection Ihre Kommunikation, sodass vertrauliche Daten nicht in falsche Hände geraten können.

Schützen Sie Ihr System vor dem Totalausfall! **Ace Backup** legt zeitgesteuert Sicherungen Ihrer wichtigsten Dateien an. Diese werden platzsparend komprimiert und auf Wunsch verschlüsselt. Ace Backup hält Ihre Archive automatisch aktuell, indem es selbstständig nach geänderten Dateien sucht und diese in das Backup integriert.

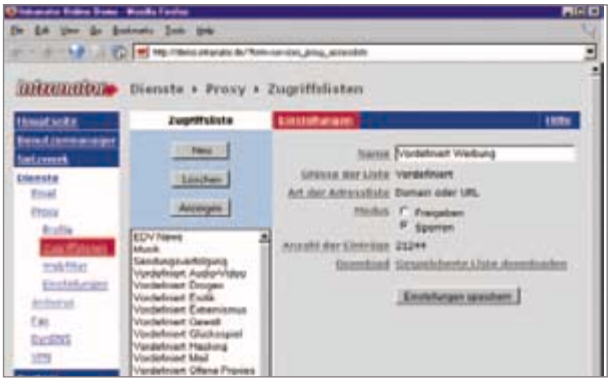
Niels Held

VOLLVERSION: INTRANATOR → Vollversionen

Linux-Server für sichere Netze

Mit der Intranator Enterprise Edition stellen Sie allen Anwendern im Netz einen sicheren Webzugang und Mailserver zur Verfügung.

Perfekter Schutz Sichern Sie Ihr Netzwerk von innen und außen: Der Intranator ist ein Security Gateway, der alle Rechner im Netz mit Internetzugang, Firewall und Mailserver samt Viren-Schutz und Spam-Filter versorgt. Den sicheren Austausch von Daten mit Rechnern außerhalb des LANs garantiert die Unterstützung von Virtual Private Networks. Über einen integrierten Proxy-Server legen Sie fest, auf welche Web-Inhalte Ihre Benutzer zugreifen dürfen. Die Bedienung erfolgt bequem per Browser. **Achtung:** Für den Intranator benötigen Sie einen eigenen Rechner, da bei der Installation die Festplatte gelöscht wird.

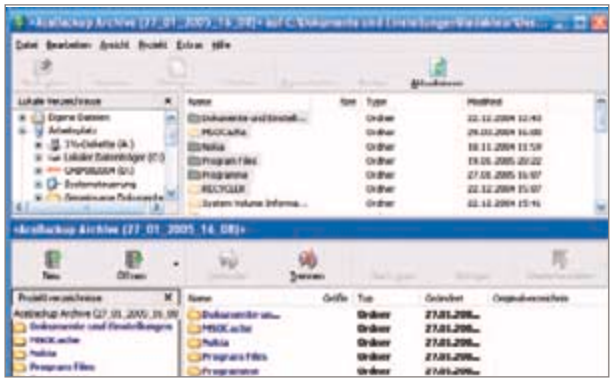


VOLLVERSION: ACE BACKUP → Vollversionen

Daten schnell & einfach sichern

Die Backup-Software Ace Backup 2003 sichert Ihre wichtigsten Daten vollautomatisch oder manuell mit Hilfe von Assistenten.

Das bessere Backup Ohne regelmäßige Datensicherung sollten Sie Ihren Rechner nicht abschalten. Ace Backup erleichtert Ihnen die leidige Aufgabe. Mit der Software legen Sie ohne Aufwand stark komprimierte Datensicherungen Ihrer wichtigsten Dateien und Ordner an und legen diese lokal oder auf einem FTP-Server im Netzwerk ab. Dank der integrierten Verschlüsselung lassen sich Ihre Backups von keinem Unbefugten auslesen. Auf Wunsch nimmt Ace Backup die Sicherungen auch zeitgesteuert vor. Dank des praktischen Assistenten finden sich sogar Einsteiger sofort in dem Programm zurecht.



MOBILE | SOFTWARE-PAKET → Blackberry

Geniale BlackBerry-Tools

Basic Facts:
→ **Mobiles Office-Paket**
→ **Datenschutz, Faxfunktion**
→ **Web, AOL und Hotmail**

Beschreibung: Auf der Heft-DVD finden Sie ausgewählte Tools für Ihren Blackberry-Handheld. Bearbeiten und erstellen Sie Word- und Excel-Dateien auch unterwegs mit eCell und eWord. eWorks verwaltet Ihre Termine, Aufgaben und Kontakte (alle in eOffice enthalten). Schützen Sie private Daten mit CryptMagic. Das Tool Mail2fax erlaubt es, Ihre E-Mails an beliebige Fax-Geräte zu senden. Der WebViewer holt Webseiten auch unterwegs auf Ihren Handheld. HotViewer und GotMailViewer zeigen Hotmail- und AOL-Mails an.

Tipp: Kostenlose Unterhaltung bietet die Software Dream Meanings Dictionary, mit der Sie Ihre Träume deuten lassen.

SNIFFER | NETSTUMBLER

Windows: Drahtlos-Netze aufspüren

Basic Facts:
→ **Spürt Wireless-Netze auf**
→ **Anzeigen von Netz-Details**
→ **Grafik der Sendeleistung**

Beschreibung: Mit der Freeware Network Stumbler finden Sie drahtlose Netze und erhalten zahlreiche Auskünfte zu Access-Point-Hersteller, MAC, Verschlüsselung und SSID. Die Empfangsstärke eines Senders gibt der Network Stumbler in einer grafischen Übersicht wieder.

Tipp: Mit einem GPS-Gerät lassen sich zusätzlich die genauen geografischen Positionen der APs abspeichern.

→ W-LAN

SNIFFER | KISMET

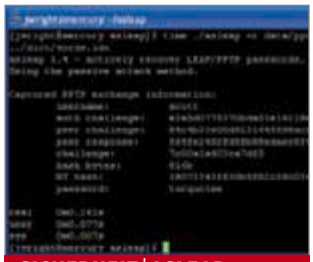
Wireless-Netze finden unter Linux

Basic Facts:
→ **Aufspüren von W-LANs**
→ **Optimieren des Standortes**
→ **Schutz vor Eindringlingen**

Beschreibung: Kismet spürt W-LANs nach dem 802.11-layer2-Standard auf. Es arbeitet vollkommen passiv und ist bei der Arbeit nicht auszumachen. Das Tool findet automatisch alle Netze in Reichweite und kann versteckte Netze oder unauthorisierte Benutzer enttarnen.

Tipp: Nutzen Sie Ethereal, um die mit Kismet abgefangenen Pakete erneut anzuzeigen und weiter zu analysieren.

→ W-LAN



SICHERHEIT | ASLEAP

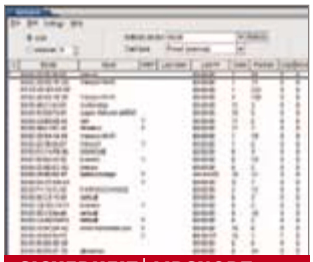
LEAP-Passwörter knacken

Basic Facts:
→ **Knackt LEAP-Passwörter**
→ **Live oder aus Capture-Datei**
→ **Aktiver Angriff möglich**

Beschreibung: Das Tool entarnt schwache LEAP Passwörter. LEAP (Lightweight Extensible Authentication Protocol) ist ein Sicherheitsmechanismus der Firma Cisco zur Authentifizierung von Anwendern und Access Points, der in den weit verbreiteten Cisco Access Points verwendet wird.

Tipp: Über den Schalter „- D“ erhalten Sie eine Auflistung der Geräte, mit denen die Live-Entschlüsselung funktioniert.

→ W-LAN



SICHERHEIT | AIRSNORT

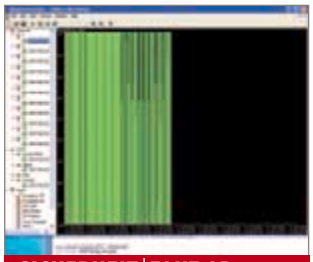
WEP-Schlüssel auf Sicherheit testen

Basic Facts:
→ **Knackt WEP-Schlüssel**
→ **Eigenes W-LAN absichern**
→ **Einfache Bedienung**

Beschreibung: AirSnort ermöglicht es, 802.11 WEP-Schlüssel zu knacken. Dazu werden Daten-Pakete des zu knackenden Netzwerks aufgefangen und daraus der Schlüssel extrahiert. So finden Sie heraus, ob der von Ihnen gewählte Schlüssel sicher ist.

Tipp: Um das Tool unter Windows auszuführen, beachten Sie die Readme.win im AirSnort-Archiv. Die nötigen Zusatz-Tools finden sie auf Heft-DVD.

→ W-LAN



SICHERHEIT | FAKE AP

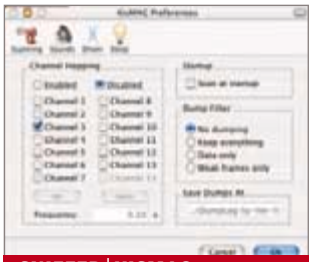
Tausende Access Points vortäuschen

Basic Facts:
→ **Schutz vor War-Drivern**
→ **Versteckt den eigenen AP**
→ **Unterstützt Honeypots**

Beschreibung: FakeAP schützt Ihr W-LAN, indem es potenziellen Angreifern tausende Access Points in der Nähe vorgaukelt. So verliert sich das echte Netz zwischen den falschen. FakeAP bietet damit ersten Schutz vor War-Drivern, Script Kiddies und anderen ungebetenen Gästen.

Tipp: Über den „-- power N“-Schalter ändern Sie die Sendeleistung einzelner APs für einen realistischeren Effekt.

→ W-LAN



SNIFFER | KISMAC

Access Points enttarnen per Mac

Basic Facts:
→ **Enttarnt Wireless-Hotspots**
→ **Analyse der Signalstärke**
→ **Umgebungskarten anlegen**

Beschreibung: KisMAC ist ein kostenloser passiver Wireless-Sniffer für MacOS X, mit dem sich W-LANs finden lassen. Da keine Anfragen von der Software gesendet werden, bleibt der Anwender von KisMAC völlig unsichtbar für andere User.

Tipp: KisMAC kann Landkarten von map24.de oder expedia.de importieren und dort gefundene APs in unterschiedlichen Farben markieren, sodass Sie diese leicht wiederfinden.

→ W-LAN

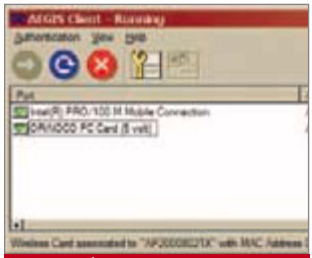
PDA-TOOLS | SOFTWARE-PAKET → W-LAN

Tool-Sammlung für Ihren PDA

Basic Facts:
→ **Schutz vor fremden Zugriff**
→ **Drahtlose Netze aufspüren**
→ **Analyse von unterwegs**

Beschreibung: Auf der Heft-DVD finden Sie eine Sammlung von Gratis-Netzwerk-Tools für Ihren PDA. Dank ständiger Verfügbarkeit erleichtern diese Tools System-Administratoren die Verwaltung drahtloser Netze. Mit den Airscanner Tools Mobile Antivirus, Firewall und Encrypter schützen Sie Ihren Pocket PC und Ihre wichtigen Daten vor fremden Zugriff. Der MiniStumbler, der Pocket Warrior und WiFiFoFum sind Sniffer für Ihren PDA, mit denen Sie W-LAN-Hotspots im Nu auffinden und analysieren können.

Tipp: Mit einer GPS-Karte für Ihren PDA, etwa von Pretec (www.pretec.com) nutzen Sie die Satelliten-gestützte Lokalisierung mit den Sniffer-Tools.



ADMIN | AEGIS CLIENT

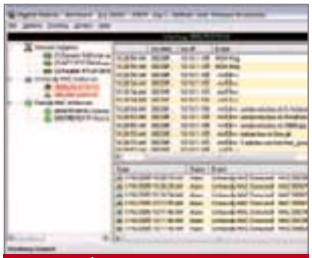
Netz vor Fremd-Zugriff schützen

Basic Facts:
→ **Sicherer Netz-Zugang**
→ **Unterstützt WPA, 802.1X**
→ **Automatisierter Login**

Beschreibung: Der AEGIS Client authentifiziert Nutzer von drahtlosen und kabelgebundenen LANs beim Login. Dazu kommuniziert die Software mit einem RADIUS- oder einem 802.1X-basierten Authentifizierungs-Server, wie etwa Microsoft IAS.

Tipp: Erstellen Sie für jede Verbindung ein eigenes Profil. Der AEGIS Client wählt später automatisch die richtigen Authentifizierungs-Daten.

→ Administration



ADMIN | AIRSNARE

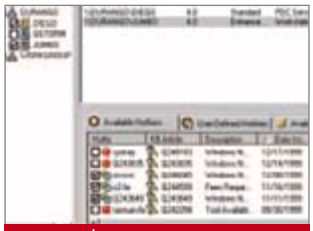
Schutz vor Daten-Dieben im LAN

Basic Facts:
→ **Eigenes Netz schützen**
→ **Web-Sitzungen aufzeichnen**
→ **Zugriffe protokollieren**

Beschreibung: AirSnare überwacht den Netzwerk-Verkehr auf so genannte „unfreundliche MAC-Adressen“ und schlägt Alarm, wenn es eine MAC-Adresse findet, die nicht in der Liste der zugelassenen Adressen ist. Zusätzlich überwacht das Tool DHCP-Anfragen von Client-Rechnern.

Tipp: Über einen Rechtsklick auf eine „Unfriendly MAC | „Send NetMsg to“ senden Sie eine Nachricht an den Nutzer.

→ W-LAN



ADMIN | SERVICE PACK MANAGER 2000

Windows-Netze aktualisieren

Basic Facts:
→ **Updates im Netz verteilen**
→ **Automatische Erkennung**
→ **Zahlreiche MS-Produkte**

Beschreibung: Der kostenlose Service Pack Manager 2000 5 User spielt Updates im Netzwerk automatisch ein. Damit erleichtert er das Beseitigen von Sicherheitslücken und Stabilitätsproblemen unter Windows NT, 2000, XP und 2003 und zahlreichen weiteren Microsoft-Produkten.

Tipp: Wählen Sie unter „Product Info“ die entsprechenden MS-Produkte aus, um Hotfixes und Infos im Web anzuzeigen.

→ Administration

ADMIN | PRTG TRAFFIC GRAPHER

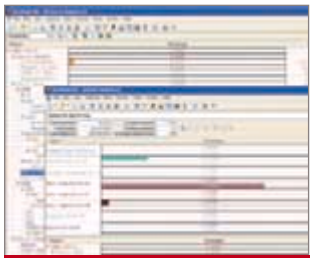
Netzwerk-Rechner schnell optimieren

Basic Facts:
→ **Echtzeit-LAN-Monitoring**
→ **Grafische Auswertung**
→ **Webserver für Fern-Zugriff**

Beschreibung: Der Paessler Router Traffic Grapher überwacht das Netzwerk, übertragenes Volumen und andere Parameter wie Speicher- und CPU-Auslastung. Das erlaubt es Admins, ihre PCs aufgabenorientiert zu optimieren. Ein integrierter Webserver erlaubt Fern-Zugriff auf die Statistiken.

Tipp: Auf der Heft-DVD finden Sie einen Schlüssel, um die Freeware für 30 Tage in die Vollversion zu schalten.

→ Administration



ADMIN | AIROPEEK SE

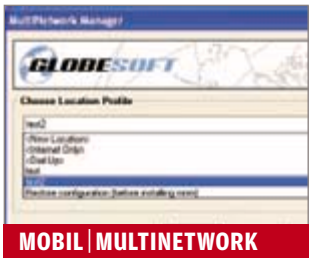
Wireless-LAN-Probleme beheben

Basic Facts:
→ **LAN-Traffic überwachen**
→ **Kennt alle 802.11-Protokolle**
→ **Echtzeit-Statistiken**

Beschreibung: AiroPeek behebt W-LAN-Probleme. Dazu erfasst es Datenpakete in Echtzeit. Unter Berücksichtigung der Signalfeldstärke, dem aktuellen Datendurchsatz und des Kanals analysiert es die Funkzellenqualität und erleichtert die Optimierung.

Tipp: Wählen Sie unter „File | New | 802.11 | Edit Scanning Options“ alle Channels und klicken Sie zweimal auf „OK“, um nach Eindringlingen zu suchen.

→ W-LAN



MOBIL | MULTINETWORK MANAGER

Netz-Anmeldung automatisieren

Basic Facts:
→ **Managt LAN-Konfiguration**
→ **Verwaltet Netz-Drucker**
→ **Erfasst System-Status**

Beschreibung: Melden Sie sich oft an verschiedenen Netzen an, müssen Sie jedesmal die Konfiguration ändern. Der Multinetwork Manager erstellt aufenthaltsort-bezogene Profile, über die Sie etwa IP-Einstellungen, Netz-Drucker oder VPN konfigurieren und wendet diese automatisch an.

Tipp: Einen einfachen Web-Zugang auf beliebigen Rechnern stellen Sie per Klick auf „Basic“ unter „Create Profile“ her.

→ Administration

SICHERHEIT | LINUX-DISTRIBUTION → W-LAN

W-LAN sichern mit Linux-Live-CD

Basic Facts:
→ **Linux-Distribution von CD**
→ **Alle Sicherheits-Tools**
→ **Analysieren und optimieren**

Beschreibung: Vier komplette Betriebssysteme finden Sie auf der Heft-DVD: Die Linux-Live-Distributionen Auditor Security Collection, PHLAK, Warlinux und Local Area Security Linux sind speziell für Sicherheits- und Administrations-Zwecke entwickelt worden. Die Versionen starten alle direkt von CD, ideal also, um flexibel W-LAN-Analysen durchzuführen, das eigene Netz auf Schwachstellen abzuklopfen oder den Standort eines Access Points zu optimieren. Alle wichtigen Tools sind bereits integriert und auf die Live-CDs angepasst worden.

Tipp: Das gewünschte Linux-Image brennen Sie mit Nero über „Datei | Öffnen | [Image-Name] | Brennen“ auf eine CD.

HOTSPOT | SNORT-WIRELESS

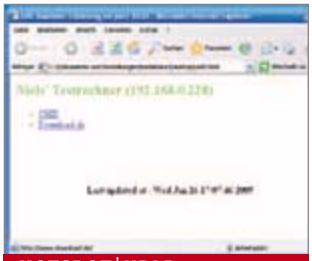
W-LAN vor Hackern schützen

Basic Facts:
→ **Schutz vor Eindringlingen**
→ **Hacker-Spuren verfolgen**
→ **W-LAN-Traffic abfangen**

Beschreibung: Snort-Wireless ist ein kostenloses Intrusion Detection System für W-LANs. Es schützt das drahtlose Netzwerk vor Eindringlingen und ermöglicht es dem Administrator, Spuren zu verfolgen. Außerdem ist Snort ein Sniffer und Packet-Logger.

Tipp: Um das Tool mit den AirJack-Treibern (auf DVD) zu verwenden, ändern Sie den ARP-Typ in der Datei airjack.c auf ARPHRD_IEEE80211.

→ W-LAN



HOTSPOT | URLD

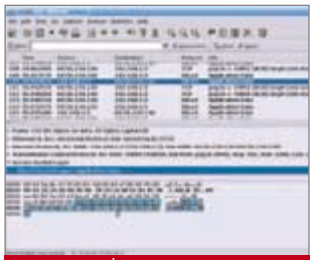
Eigenen Access Point promoten

Basic Facts:
→ **Hotspots publik machen**
→ **Link-Versand per Funk-Netz**
→ **Für alle Browser**

Beschreibung: Urld verbreitet Weblinks innerhalb einer Wireless-Domäne oder -Zelle. Anwender, die in Reichweite der Zelle kommen und auch urld verwenden, erhalten automatisch die ausgestrahlten Weblinks zugesandt. Diese werden in einer HTML-Datei beim Empfänger gespeichert.

Tipp: Um den Speicherort der HTML-Datei zu ändern, passen Sie in der Datei „urld.conf“ den Eintrag hinter „recv“ an.

→ W-LAN



ANALYSE | ETHEREAL

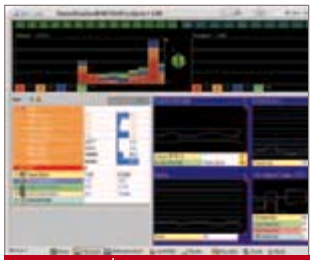
W-LAN-Verkehr analysieren

Basic Facts:
→ **Analyse und Fehlersuche**
→ **Datenpakete abfangen**
→ **Kennt über 650 Protokolle**

Beschreibung: Ethereal bietet detaillierte Netzwerk-Analyse auf Protokoll-Ebene. Dazu fängt es den Datenverkehr im Netzwerk ab oder liest Daten-Logs, die etwa mit Kismet erzeugt wurden, aus. Die Daten lassen sich im Text-Modus betrachten und ausdrucken.

Tipp: Um mit der Windows-Version Datenpakete abfangen zu können, installieren Sie vorher die WinPcap-Bibliothek von der Heft-DVD.

→ Administration



ANALYSE | AIRMAGNET

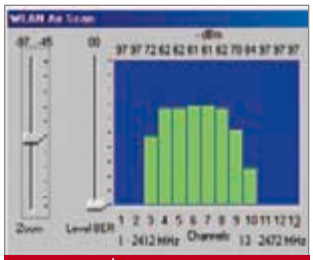
Drahtlose Netze überwachen

Basic Facts:
→ **Automatische LAN-Analyse**
→ **Erkennt 100+ LAN-Probleme**
→ **Wireless Troubleshooting**

Beschreibung: Die Software erfasst automatisch kritische Informationen über Ihr W-LAN und stellt anschließend detaillierte Ergebnisse zur Verfügung. So ermöglicht der Laptop Analyzer einfache Netzwerk-Verwaltung und erleichtert die LAN-Optimierung.

Tipp: AirMagnet benötigt spezielle W-Lan-Karten-Treiber, die Sie über das „Laptop Demo Update Tool“ in der AirMagnet-Programmgruppe installieren.

→ W-LAN



ANALYSE | WLAN EXPERT

Wireless-Netze optimieren

Basic Facts:
→ **W-LAN-Störquellen orten**
→ **Hotspot-Standort ermitteln**
→ **Grafischer Antennentest**

Beschreibung: WLAN Expert zeigt die Signalstärke, Fehler und Interferenzen bei Verbindungen zu einem W-LAN-Netz an. Mit Hilfe eines grafischen Antennen-Tests lässt sich die Qualität des Funk-Signals ermitteln und so gegebenenfalls ein besserer Standort wählen.

Tipp: Über „Tx Power“ verringern Sie die Sendeleistung – ideal um etwa die Reichweite Ihres W-LAN-Adapters auf die Wohnung zu beschränken.

→ W-LAN

HOTSPOT | CQURE AP

Mini-Hotspot von Diskette starten

Basic Facts:
→ **Vollständiger Access Point**
→ **Benötigt nur 1,44 Megabyte**
→ **DHCP, Firewall, 802.1X**

Beschreibung: Cqure AP ist ein Wireless Access Point, der auf einer winzigen Linux-Distribution läuft. Das Tool startet von einer einzigen Diskette. Die Software lässt sich als Bridge oder Gateway konfigurieren und bietet einen DHCP-Server, eine Firewall und unterstützt 802.1X-Authentifizierung.

Tipp: Benutzen Sie das Tool RawWrite (DVD-Code: Windows-Basics), um das Image auf eine Diskette zu schreiben.

→ W-LAN

Die Zukunft drahtloser Netzwerke

WiMAX: Das Super-W-LAN

Aktuelle W-LAN-Netzwerke stoßen bei Datenraten von 54 MBit/s und Reichweiten von 200 Metern an ihre physikalischen Grenzen. Die zukünftige Breitbandtechnik WiMAX dagegen soll mit bis zu 75 MBit/s noch in Entfernungen von 50 Kilometern funken – und damit die 250fache W-LAN-Reichweite bieten.

In der Kleinstadt Selm in Nordrhein-Westfalen bahnt sich Großes an: Der 30.000-Einwohner-Ort könnte bald zum Mekka für Netzwerk-Freaks werden. In einem Pilotprojekt will Selm als erste deutsche Stadt die neue Funktechnik WiMAX („Worldwide Interoperability for Microwave Access“) testen.

Die enormen Vorteile: Mit WiMAX lassen sich Entfernungen von bis zu 50 Kilometern überbrücken – bei Bandbreiten von bis zu 75 MBit/s. Damit avanciert WiMAX nicht nur zum Konkurrenten von W-LAN, sondern bietet sich auch dort als Alternative zu DSL-Netzen an, wo aus Kostengründen auf eine Verkabelung der „letzten Meile“ verzichtet wurde. Die Vision, selbst in den abgelegensten Gegenden mit Highspeed durchs Internet zu surfen, könnte mit WiMAX Wirklichkeit werden.

WiMAX: Die Entwicklung des neuen Funkstandards

WiMAX ist aus der Spezifikation IEEE-802.16 entstanden (siehe Tabelle unten). Dieser Richtfunkstandard wurde 2001 für das Metropolitan Area Network (MAN) konzipiert, also für die Datenübertragung in Großstädten über eine direkte Sichtverbindung („Line Of Sight“, LOS).

Anfang 2003 kam ein neuer Impuls: Mit der Idee, diesen Standard auch für portable Endgeräte zu nutzen, entstand unter der Federführung von Intel das WiMAX-Forum, dem mehr als 200 Technologie-Unternehmen angehören, darunter Konzerne wie Siemens mobile, Fujitsu, AT&T, British Telecom und Nokia.

Noch im gleichen Jahr verabschiedete das Forum die Standards 802.16a und 802.16REVd – WiMAX war geboren. Beide Spezifikationen wurden im Juli 2004 zum 802.16-2004-Standard zusammengefasst. Dabei werden erstmals NLOS-Verbindungen („Non Line Of Sight“) berücksichtigt: Daten können somit auch über Hindernisse hinweg übertragen werden. Die Antenne des Empfängers ist dazu entweder an der Außenwand oder innerhalb des Hauses montiert.

Mit der nächsten WiMAX-Ausbaustufe 802.16e werden ab 2006 auch mobile Endgeräte wie PDAs, Handys oder Notebooks unterstützt – inklusive Roaming (also Kommunikation der Geräte untereinander). Dabei sollen bis zu 15 MBit/s Bandbreite und Reichweiten bis zu fünf Kilometern erreicht werden.

Um diese Datenraten und Reichweiten bieten zu können, setzt WiMAX auf gravierende Neuerungen im Vergleich zum Vorgänger WiFi („Wireless Fidelity“, umfasst die W-LAN-Standards 802.11a/b/g). Ein großer Unterschied ist etwa die Möglichkeit des „Beam Shaping“. Der Clou: Um die Richtcharakteristik einer typischen WiMAX-Basisstation, die aus mehreren Sendeantennen besteht, auf die benötigte Reichweite und Bandbreite einzustellen, lassen sich alle Antennen miteinander koppeln – ohne Mechanik. Allein die elektromagnetische Variation der Antennenleistung bestimmt die Richtcharakteristik.

Um Daten sicher zu übertragen, nutzt WiMAX das so genannte OFDM-Verfahren („Orthogonal Frequency Division Multiplexing“, siehe Grafik rechts). Dabei findet die Modulation der Trägersignale parallel und nicht wie üblich seriell statt. Dadurch bleiben die Informationen, die jedes einzelne parallele Trägersignal transportiert, gegenüber einem seriellen Single-Carrier-Verfahren in der Luft länger stabil.

Das ist wie bei einer mehrspurigen Autobahn: Fällt eine Spur aus, fließt der Verkehr über die anderen freien Fahrbahnen weiter. Für die Datenübertragung heißt das: Wird das Trägersignal durch Laufzeiteffekte (Mehrfachreflexionen oder fehlende Richtcharakteristik) geschwächt, stehen OFDM mehr Frequen-

DAS LEISTEN DIE VERSCHIEDENEN IEEE-802.16-STANDARDS

Bezeichnung	IEEE 802.16	IEEE 802.16a/REVd/2004 (WiMAX)	IEEE 802.16e (WiMAX)
Frequenzband	10 bis 66 GHz	2 bis 11 GHz	0,7 bis 6 GHz
Bedingung für eine Übertragung	Direkte Sichtverbindung von Sender und Empfänger (LOS)	Direkte oder indirekte Verbindung von Sender und Empfänger (NLOS)	Direkte oder indirekte Verbindung von Sender und Empfänger (NLOS)
Max. Bitrate	Variabel, mehrere 100 MBit/s	75 MBit/s	15 MBit/s
Modulationsart	QPSK, 16 QAM und 64 QAM	OFDM 256, OFDMA 64 QAM, 16 QAM, QPSK, BPSK	OFDM 256, OFDMA 64 QAM, 16 QAM, QPSK, BPSK
Position der Empfängereinheit	Fest, unbeweglich	Fest und „eingeschränkt beweglich“	Fest bis mobil
Maximale Reichweite	Variabel, bis über 100 Kilometer	Rund 50 Kilometer	Rund fünf Kilometer
Geräte, Verfügbarkeit	Keine Bedeutung für Consumer-HW, ab sofort verfügbar	Basisstationen, System-on-a-Chip, ab Anfang 2005	Handy, PDA, Notebook, ab Anfang 2006

Die besten WiMAX-Tipps im Web

Wissen aus erster Hand → www.wimaxforum.org
Hier informieren die WiMAX-Förderer über die Funktechnologie
WiMAX in der Praxis → http://wimax-selm.de/
Auf dieser Seite können Sie den WiMAX-Test in Selm live verfolgen

zen als „Fahrbahnen“ zum Ausweichen zur Verfügung. Das schlägt sich in höherer Reichweite und Bitrate nieder.

Ein 802.16a-System ist typischerweise in fünf Kanäle à 20 MHz in einem Frequenzband von 5,725 bis 5,825 GHz unterteilt. Jeder dieser 20 MHz breiten Kanäle kann etwa 75 MBit/s Bandbreite bereitstellen. Im Beispiel entspricht das einer fünfspurigen Autobahn. Die theoretische Kapazität des kompletten 100-MHz-Bands beträgt damit sogar 375 MBit/s.

Mit der „Adaptiven Modulation“ verfügt WiMAX über eine Technik, mit der sich je nach Verbindungsqualität verschiedene Modulations-Schemata nutzen lassen. So schaltet der Sender etwa bei hoher Qualität auf das 64-QAM-Verfahren (6 Bit Information pro Trägersignal), bei schlechter Signal-Qualität dagegen auf das BPSK-Verfahren (binäre Phasen-Modulation), das sicheren Empfang bei geringen Bitraten garantiert.

Bald erhältlich: Die ersten WiMAX-Geräte

Im Rahmen des Intel Developer Forums (IDF) im September 2004 in San Francisco hat Intel erstmals technische Details für WiMAX-Produkte bekanntgegeben. „Rosedale“ heißt beispielsweise der erste „System-on-a-Chip“-Baustein, der eine drahtlose Breitband-Internetverbindung über eine Entfernung von bis zu 50 Kilometer zu Firmengebäuden oder Privathaushalten herstellen kann. Rosedale wird in ortsfesten Basisstationen sitzen und den aktuellen WiMAX-Standard 802.16-2004 unterstützen.

Von der letzten WiMAX-Ausbaustufe 802.16e sollen PDAs, Handys oder Notebooks profitieren. Erste Geräte werden für 2006 erwartet, den großen Durchbruch soll es mit dem Notebook-Chipsatz „Calexico 3“ geben: Er arbeitet nach dem 802.16e-Standard und ermöglicht so im mobilen Betrieb eine kabellose Breitbandverbindung.

Die Zukunft von WiMAX: Selm ist erst der Anfang

WiMAX kann die Netzwerkstruktur der Zukunft grundlegend umkrempeln. Die möglichen Bitraten sind um den Faktor 200 höher als die von UMTS (384 KBit/s); selbst der schnellste derzeit kommerziell verfügbare DSL-Standard erreicht mit etwa 3 MBit/s gerade mal ein Fünftel des 802.16e-Standards.

Trotz all dieser Vorteile gibt es einige Hindernisse: In Ländern wie Deutschland, in denen es bereits eine hohe Verkabelungsdichte (DSL-/Telefonleitung) gibt, wird es WiMAX schwer haben, sich durchzusetzen. Selbst der Innenraum einer Wohnung, in den WiMAX mit seiner letzten Ausbaustufe (802.16e) vorstoßen will, wird schon heute mit W-LAN abgedeckt.

Dennoch wird es Bereiche geben, in denen WiMAX seine Stärken ausspielen kann – besonders dort, wo es aufgrund der Infrastruktur nicht möglich ist, DSL-Leitungen kostengünstig zu verlegen. Von WiMAX profitieren werden Länder, die bislang noch nicht engmaschig verdrahtet sind. China, Indien oder Russland stehen ganz oben auf der WiMAX-Prioritäts-Liste.

KNOW-HOW

So funktioniert WiMAX

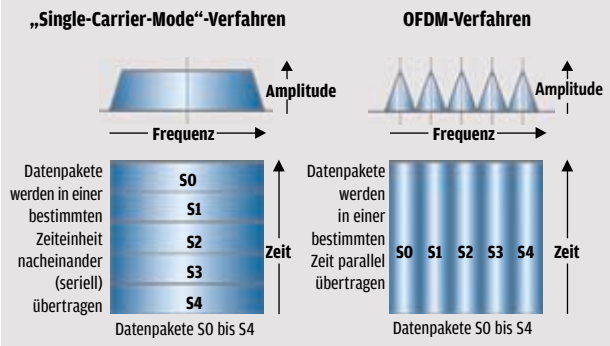
Wie bei allen Funktechnologien muss sich auch WiMAX der Physik der Hochfrequenztechnik beugen. Dennoch gibt es einige wegweisende Neuerungen.

WiMAX ist auf die Art des Senders (Richtantenne) und deren Standort (Außenwand, hohe Gebäude) optimiert. Daneben wird die typische Strahlungskeule einer HF-Sendeantenne über das neue Beam-Shaping-Verfahren beeinflusst. So können ab dem Standard 802.16a Antennen einer Basisstation gekoppelt werden, um ihre Richtcharakteristik auf Reichweite und Bandbreite anzupassen. Das Besondere: Einzig durch elektromagnetische Variation der Antennenleistung wird die Richtcharakteristik verändert.

Neu ist auch die Art der Datenübertragung. Per OFDM-Modulation findet die Modulation des Trägersignals parallel und nicht wie bisher üblich seriell statt. Die Informationen, die das parallele Trägersignal transportiert, bleiben so länger stabil in der Luft. Bei Abschwächungen durch Mehrfachreflexionen, fehlende Richtcharakteristik oder Wände bleiben Datenübertragungen damit länger stabil, was sich in einer höheren Reichweite und Bitrate niederschlägt.

Neben OFDM verwendet WiMAX die Adaptive Modulation, die abhängig von der Qualität der Verbindung (SNR, Signal to Noise Ratio) verschiedene Modulations-Schemata verwendet. So schaltet der Sender bei einem hohen SNR-Pegel (sehr guter Link) auf das hochwertige 64-QAM-Verfahren (6 Bit Information pro Trägersignal), während er bei einer schlechten Signalqualität auf das BPSK-Verfahren (binäre Phasen-Modulation) zurückgreift, was für einen sicheren Empfang bei kleineren Bitraten sorgt.

OFDM: Parallel statt seriell



OFDM-MODULATION: Wird das Trägersignal geschwächt, etwa beim Durchdringen von Wänden, lässt es sich wegen der „längeren Gültigkeit“ leichter zurückgewinnen.

Illustration CHIP

Dass Funktechnologien wie W-LAN und WiMAX einander nicht ausschließen, sondern vielmehr sinnvoll ergänzen, zeigt bereits ein einfaches Beispiel: Während eine WiMAX-Basisstation für einen Verbindungsaufbau bis an die Außenwand eines Gebäudes sorgt, wird die Signalübertragung über eine Leitung an einen ganz normalen IEEE-802.11-W-LAN-Router innerhalb des Hauses sichergestellt – einfacher geht’s nicht! So könnten neben der nordrhein-westfälischen Kleinstadt Selm auch andere „Insel-Städte“ in naher Zukunft von dem drahtlosen Netzwerk WiMAX profitieren.

Daniel Bader

Umstrittene Wireless-Technologie

Das Potenzial von RFID

Radio Frequency Identification (RFID) ist auf dem besten Weg, zum Reizwort zu werden. Denn in den winzigen Chips mit Abmessungen von wenigen Millimetern erkennen viele das Ende des Datenschutzes und den Verlust zahlloser Arbeitsplätze im Einzelhandel. CHIP zeigt Ihnen, was hinter RFID steckt.

Die RFID-Technologie ist seit mehr als 20 Jahren in Warensicherungssystemen großer Kauf- und Warenhäuser im Einsatz. Jedermann bekannt sind die Bügel im Bereich des Kassenausgangs und die Gesten des Kassenpersonals, die eine Ware entweder über ein spezielles Gerät reiben oder schlicht und einfach ein kleines Modul von der Ware entfernen. An dieser Stelle handelt es sich um vergleichsweise simple Ein-Bit-Transponder. Etwas komplexer sind dagegen Transponder mit Speicherkapazitäten von bis zu 64 KByte – das entspricht immerhin dem Speicherplatz eines C64-Heimcomputers aus den achtziger Jahren –, die sich darüber hinaus auch über die Funkschnittstellen mit Daten beschreiben lassen.

Datenschützer sehen dabei in erster Linie das Risiko des unbemerkten Anlegens von Bewegungsprofilen sowie der unkontrollierbaren Speicherung personenbezogener Daten – um so mehr, als die Übertragung der Daten kontaktlos erfolgt und theoretisch völlig unbemerkt möglich ist.

RFID: Vielfältige Wireless-Technologie

Der Begriff RFID beschreibt eine sehr komplexe Technologiefamilie und keinesfalls einen einzigen Standard. Die Systeme unterscheiden sich in ihrer Reichweite, in der Betriebssfrequenz und in der Art des Informationsaustauschs.

Close-Coupling-RFID-Systeme etwa haben eine sehr kurze Reichweite von nur wenigen Zentimetern. Derartige Systeme kommen für Zugangskontrollen und Kfz-Wegfahrsperren zum Einsatz. Aus der Sicht des Datenschutzes ist wichtig, dass diese Transponder eine direkte Interaktion dessen erfordern, der sich mit ihrer Hilfe authentifizieren möchte. Keinesfalls können Close-Coupling-Systeme unbemerkt mit Hilfe eines versteckten Lesegerätes ausgewertet werden. Der Vorteil der RFID-Technologie ist die robuste Bauform der Transponder, deren Funktion nicht durch Schmutz oder Feuchtigkeit beeinträchtigt werden kann. Die Energieversorgung und die Übertragung der Daten kann entweder induktiv oder kapazitiv erfolgen.

Remote-Coupling-Systeme lassen dagegen Betriebsdistanzen von bis zu 150 Zentimetern zu. Die bekannten Warensicherungssysteme gehören zu dieser Familie. Die Kopplung zwischen Transponder und Lesegerät erfolgt in der Regel induktiv. Die gängigsten Betriebsfrequenzen liegen im langwelligen Bereich um 135 kHz, im Kurzwellenbereich um 13,56 MHz.

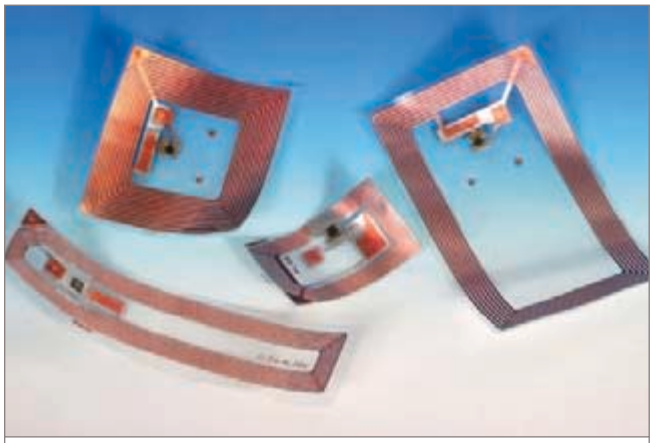
Lediglich so genannte Long-Range-Systeme erlauben Distanzen von etwa zehn Metern zwischen dem Transponder und dem Lesegerät. In dieser Entfernung ist keine Kopplung über das magnetische Feld der Lesespule mehr möglich. Es handelt sich meist entweder um so genannte aktive RFID-Transponder, die mit einer eigenen Batterie ausgerüstet sind, oder um passive Modelle mit einer Stützbatterie. Long-Range-Systeme arbeiten meist im UHF- oder im Mikrowellenbereich.

Zu unterscheiden sind – wie schon angedeutet – auch aktive Transponder, die mit einer eigenen Batterie ausgestattet sind und damit auch große Distanzen mit eigener Sendeleistung überwinden können, und passive Transponder. Passive Transponder beziehen ihre Betriebsenergie aus dem Feld des Lesegerätes oder beeinflussen durch ihre Resonanz- oder Reflexionseigenschaften passiv die Energieverhältnisse des Lesegeräts.

Beispiel: RFID-System mit Lastmodulation

RFID-Transponder – insbesondere passive Transponder ohne eigene Energieversorgung – sind nicht mit leistungsstarken Sendeendstufen zu realisieren. Man muss daher andere Wege finden, um die Informationen des Transponders an das Lesegerät zu übertragen.

Ein Beispiel ist die so genannte Lastmodulation, deren Grundprinzip die Veränderung eines frequenzabhängigen Widerstands innerhalb des Feldes eines Lesegeräts ist. In der einfachsten Form stellt der Transponder einen Schwingkreis dar, dessen Resonanzfrequenz der Sendefrequenz des Lesegeräts entspricht. Gelangt dieser Transponder in das Feld des Lesegeräts, stellt der geringe Widerstand des in Resonanz befindlichen Kreises eine Last für das Feld dar, was in der Form eines Spannungsabfalls an der Spule des Lesegeräts messbar ist. Durch den Kurzschluss des Schwingkreises im Transponder im Takt der zu übermittelnden Informationen verändert sich



RFID-TRANSPONDER: Die Mini-Funkchips lassen sich – als Klebefolie gefertigt – problemlos in Bücher, Aktendeckel und sogar Preisetiketten integrieren.

diese Lastsituation und damit auch der Spannungsabfall an der Spule des Lesegeräts.

Das Feld des Lesegeräts ist sehr stark und damit extrem dominant gegenüber der vergleichsweise kleinen Laständerung durch den winzigen Transponder. Aus diesem Grunde kommt in der Praxis meist eine Sonderform der Lastmodulation zum Einsatz, bei der man sich einen Effekt zunutze macht, der durch das Grundprinzip der Amplitudenmodulation begründet ist. Bedingt durch die Veränderung des Signals in der Amplitude und damit auch durch die Abweichung von der ursprünglichen Spektralform entstehen neue Signale in den so genannten Seitenbändern. Solche Seitenbänder lassen sich definiert erzeugen, wenn die Resonanzeigenschaften des Transponder-Schwingkreises mit einer bestimmten Frequenz gesteuert werden. Damit schwanken auch die Spannungsänderungen an der Spule des Lesegeräts minimal im Takt dieser Frequenz, die jedoch – weil sie per Definition bekannt ist – einfach herausgefiltert werden kann. Die eigentlichen Nutzinformationen, die im Transponder gespeichert sind, werden nun vor der Ansteuerung des Schwingkreises auf diesen Hilfsträger aufmoduliert. Bei der Wahl des Modulationsverfahrens gibt es verschiedene Optionen, beispielsweise Amplituden-, Frequenz- und Phasenumtastung. Wichtig ist jedoch, dass Transponder und Lesegerät jeweils dieser Vereinbarung entsprechen.

Weil ein Hilfsträger mit bekannter Frequenz sehr einfach – auch aus einem dominanten Signal mit sehr hohem Pegel – herausgefiltert werden kann, lassen sich die Informationen des Transponders nach Verstärkung und Demodulation des Hilfsträgers mit großer Zuverlässigkeit wiederherstellen und interpretieren. Das Verfahren eignet sich ausgezeichnet zum Lesen von Transpondern mit einer Informationsmenge von mehreren Bit. Es kommt in Systemen mit kurzer bis mittlerer Reichweite (bis etwa 150 Zentimeter) zum Einsatz.

RFID ganz praktisch: Tiere identifizieren

Eine bereits häufig genutzte Anwendung der RFID-Technologie ist die Tieridentifikation. Dabei wird dem Tier (beispielsweise einem Hund oder einer Katze) ein Transponder mit den Abmessungen von etwa 12 x 2 Millimeter unter das Fell injiziert. Das Verfahren gilt als schmerzlos und ist in jedem Fall als humaner einzustufen als die Tätowierung, wie sie schon seit einiger Zeit bei Rassetieren üblich ist.

Die Kennzeichnung des Tieres durch den Chip stellt einen eindeutigen Bezug zu dessen Papieren her. Darüber hinaus kann mit Hilfe von RFID – der entsprechende Eintrag in eine zentrale Datei vorausgesetzt – ein entlaufenes Tier rasch seinem Eigentümer zurückgegeben werden. Das ist nicht nur schön für den Besitzer, sondern hat auch wirtschaftliche Bedeutung, denn das Verwahren von Tieren unbekannter Eigentümer ist auf die Dauer sehr teuer.

Nicht zuletzt weist der Hersteller von Tierarzneimitteln, die Virbac GmbH aus Bad Oldesloe, auf die aktuellen EU-Verordnungen hin, die neben einem EU-weit einheitlichen Tierpass auch deren Kennzeichnung mit einem RFID-Transponder vorsehen. Tätowierungen von Haustieren werden nur noch für eine begrenzte Übergangszeit geduldet.

Robert Schoblick

KNOW-HOW

Der Supermarkt der Zukunft

RFID kann in der Logistik- und Einzelhandelsbranche viele Arbeitsplätze kosten. Kassensysteme im Supermarkt lassen sich durch RFID weitgehend automatisieren und die Planung der Warenplatzierung in Verkaufsregalen von zentraler Stelle aus managen.

Ganz ohne Personal wird der Supermarkt der Zukunft zwar nicht auskommen, doch ist es sehr wahrscheinlich, dass für einen Markt viel weniger Mitarbeiter nötig sind als heute. So wird es zu den Kerntätigkeiten eines Verkäufers gehören, die Regale nach zentralen Anweisungen aufzufüllen und die Kunden zu beraten. Allerdings werden Multimedia-Info-Terminals die eigentlichen Produktinformationen sowie Daten zur Verfügbarkeit und zu Lieferfristen bereitstellen.

Über die mittleren Reichweiten der Transponder an den Waren lassen sich Wareneingänge und -ausgänge in Echtzeit erfassen, Nachbestellungen erfolgen automatisch.

Der Weg der Waren lässt sich mit Hilfe von RFID von der Herstellung bis zum Verkauf lückenlos protokollieren. Die Waren werden auf Paletten und in Container verladen, die ihrerseits mit RFID-Transpondern großer Reichweite (etwa zehn Meter) versehen sind. Sie werden bei den Be- und Entladevorgängen gelesen und dem jeweiligen Transportmittel in einer Datenbank zugeordnet. Mit Hilfe zusätzlicher Tracking-Daten – etwa GPS-basierende Positionsdaten eines Lkws oder Waggons – lässt sich damit jederzeit feststellen, wo sich die Sendung gerade befindet. Lieferverzögerungen aufgrund von Verkehrsengpässen oder Verspätungen kann der Händler sofort erkennen und entsprechend den weiteren Verlauf einer Projektbearbeitung kalkulieren.

Gläserner Kunde dank RFID?

Bereiten die „Schnüffel-Chips“ dem gläsernen Kunden endgültig den Weg? Tatsache ist: Die RFID-Transponder können unter bestimmten Voraussetzungen, aber eben stets nur im Bereich ihrer Betriebsreichweite, heimlich – also unbemerkt vom Träger des Transponders – ausgelesen werden. Bei Close-Coupling-Systemen ist dagegen ein heimliches Auslesen nahezu unmöglich. Das gilt unter anderem für elektronische Pässe, möglicherweise eines Tages verfügbare Banknoten mit RFID-Chip und für Zugangsausweise.

Warensicherungssysteme arbeiten bereits seit Jahren mit RFID, speichern aber meist nur ein einziges Bit. Die nächste Generation wird jedoch Artikelnummern erkennen können. Auch das ist im Vergleich zu heute bereits etablierten Verfahren weitgehend unkritisch. Werden jedoch weltweit einmalige Seriennummern in den Chip implementiert, bedeutet dies, dass der Kunde auf seine Anonymität verzichten muss.

Mit einem Barcode sind schon heute alle Waren versehen. Er stellt eine eindeutige Zuordnung zum Artikel, jedoch keine individuelle Seriennummer dar. Authentifiziert sich ein Kunde durch Kundenkarte, Kredit- oder EC-Karte, ist es möglich und nach Genehmigung des Kunden auch üblich, dass die Einkäufe personalisiert werden. Damit lassen sich Verhaltensmuster anlegen, anhand derer die Wirkungen von Umorganisationen, Sortimentsänderungen und Sonderaktionen bewertet werden können. Personalisierte Werbung wird damit preiswerter und erfolgreicher.

Kritisch sind auch personalisierte RFID-Fahrausweise in öffentlichen Verkehrsmitteln zu sehen, die das Anlegen von Bewegungsprofilen des Fahrgastes ermöglichen.

W-LAN AUFBAUEN | INHALT

Die richtige Hardware 44
Ein Funknetzwerk lässt sich ganz leicht aufbauen, wenn die richtige Hardware verwendet wird.

Die Antenne macht's 50
Wer die Reichweite seines Funknetzes erhöhen will, sollte sich eine externe Antenne zulegen.

W-LAN unter XP einrichten 52
In wenigen Schritten konfigurieren Sie Ihr drahtloses Netzwerk unter Windows XP.

Ressourcen freigeben 58
Alles teilen: So geben Sie den Internet-Zugang, Dateien und Drucker für alle Nutzer frei.

Die funkende Ich-AG 62
Surfen und arbeiten in den eigenen vier Wänden – so richten Sie sich ein Wireless Home Office ein.

W-LAN aufbauen mit Linux 64
Mit SuSE Linux 9.2. lässt sich ein drahtloses Funknetzwerk endlich komfortabel einrichten.

In einem Wireless LAN gibt es keinen Kabelsalat. Trotzdem benötigen Sie spezielle Hardware, damit es in Ihrem Netzwerk richtig funkt. Hier erfahren Sie alles über Access Points, Funknetzwerkkarten und was Sie sonst noch für Ihr W-LAN brauchen.

CHIP AUTOR → www.goldmann.de

Martin Goldmann, Programmierer und Journalist, ist Mitinhaber des Internet-Dienstes Tippscout.de und spezialisiert auf die Programmierung von Web-Auftritten in PHP. Darüber hinaus hat er sich als Spezialist für Linux- und Wireless-Themen einen Namen gemacht.

CHIP → DVD-CODE W-LAN

- → **Software-AP** Cqure AP ist ein winziger Access Point auf Linux-Basis, der von einer Diskette startet. Er bietet DHCP, Firewall und 802.1X-Unterstützung.
- → **Pocket-Sniffer** WiFiFoFum für den Pocket PC findet sämtliche Access Points in Reichweite und zeigt diese in einer Liste mit allen wichtigen Zusatz-Infos an.
- → **LAN-Sperre** Mit AirSnare schützen Sie Ihr Netz: Die Software überwacht das LAN auf unbekannte MAC-Adressen und schlägt bei unerlaubten Zugriff Alarm.

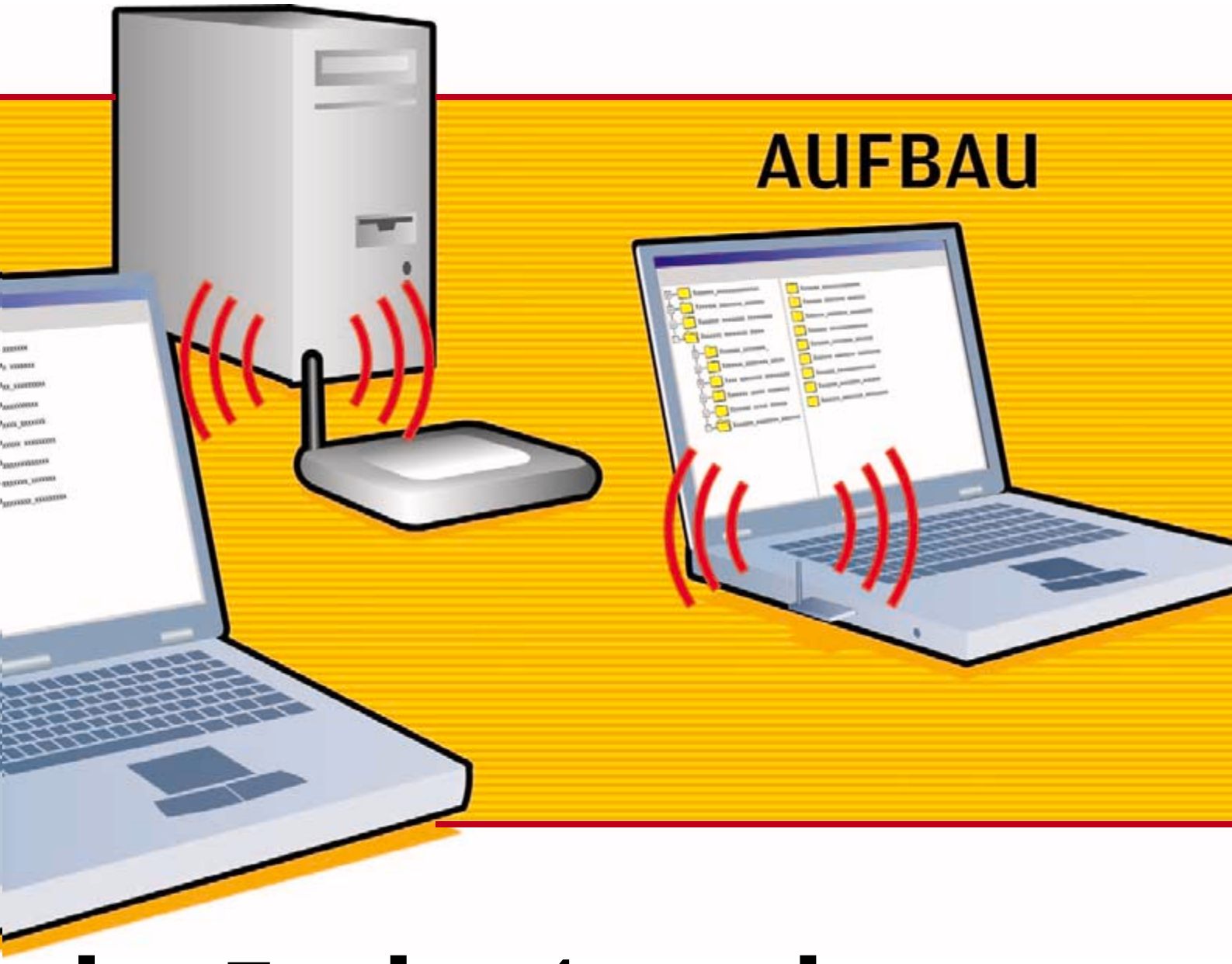
Drahtlose Freiheit

Hardware für

Sie wollen im Internet surfen oder Ihre E-Mails lesen, während Sie mit dem Notebook im Coffee-Shop sitzen? Oder möchten Sie sich zuhause oder im Büro mal eben ins drahtlose Netzwerk einklinken? Am Flughafen ganz schnell ein Meeting-Protokoll versenden? Das ist alles kein Problem, wenn Sie die richtige Hardware besitzen. In diesem Beitrag erfahren Sie detailliert, welche Geräte Sie für den Aufbau eines drahtlosen Netzwerks benötigen. Die Tabelle auf 46 gibt Ihnen einen kompakten Überblick über die in einem IEEE-802.11-W-LAN verwendeten Geräte.

Access Point: Die Basisstation

Im einfachsten Fall besteht die W-LAN-Hardware aus einer Funknetzwerkkarte und einem zentralen Access Point (AP). Ein Access Point ist ein Gerät, das ähnlich wie ein Hub im leitungsgebundenen Ethernet funktioniert. Allerdings müssen Access Points nicht zwangsläufig Hardware sein, es gibt auch Software-Lösungen, die jedoch nicht allzu weit verbreitet sind.



das Funknetzwerk

Die Besitzer von Apple-Macintosh- und Windows-Computern haben die Möglichkeit, einen Rechner mit einer Funknetzwerkkarte in einen Software-Access-Point umzuwandeln, ohne dass der normale Desktop- oder Server-Betrieb gestört wird. Diese Maßnahme erspart in manchen Fällen die Anschaffung eines Hardware-Access-Points, allerdings muss der Rechner dafür immer in Betrieb sein – mit dem vollen Risiko eines Absturzes und eines temporären Ausfalls des Netzwerks.

Eine andere Aufgabe des Access Points ist die Verbindung eines drahtlosen Netzwerks mit einem leitungsgebundenen Netz. Moderne Access Points unterstützen das Wireless Distribution System (WDS), das es den Geräten ermöglicht, gleichzeitig als Bridge und Access Point für drahtlose Clients zu agieren. Einige Access Points arbeiten auch noch als Relaisstation zwischen zwei oder mehreren anderen Access Points.

Sicher gehört die gemeinsame Nutzung der Netzwerk-Ressourcen und eines Internet-Zugangs zu den wesentlichen Vorzügen eines W-LANs. Deshalb sind fast alle Access Points mit einem Ethernet-Port und einem internen Modem zur Einwahl ins Internet ausgestattet. Erfolgt der Online-Zugang über eine Breitbandverbindung, wird das Kabelmodem oder das DSL-Modem mit dem Ethernet-Port des Access Points verbunden. Erfolgt die Internet-Einwahl dagegen per Telefon, wird das analoge Modem an den Access Point angeschlossen.

Gleichgültig, auf welchem Weg die Internet-Verbindung zustande kommt, in allen Fällen agiert der Access Point als Gateway, er verbindet das W-LAN beziehungsweise LAN mit dem Internet. Auch bestimmte Netzwerkdienste wie DHCP (Dynamic Host Configuration Protocol) und NAT (Network Address Translation) können zu den Aufgaben eines Access Points gehören. Einige Geräte bieten darüber hinaus erweiterte Features wie Paketfilter, Firewall oder Router oder unterstützen Virtual Private Networks (VPN).

Ein Access Point ist außerdem für die Sicherheit in einem W-LAN verantwortlich. Mit Hilfe eines Authentifizierungsverfahrens gewährt oder verweigert er den Zugang zum draht- →

losen Netzwerk. Unterschiedlich starke Verschlüsselungstechniken wie Wireless Equivalent Privacy (WEP) oder Wi-Fi Protected Access (WPA) sorgen für die Codierung der drahtlos gesendeten Signale.

Ein Access Point ist eine aktive Netzwerkkomponente. Im Gegensatz zu passiven Komponenten wie beispielsweise Kabeln oder Hub in einem Ethernet hat ein Access Point die Fähigkeit, Netzwerkdaten eigenständig zu verarbeiten. An einem Access Point können sich beliebig viele W-LAN-Clients (Endgeräte) einbuchen und über diesen Access Point gegenseitig alle Arten von Daten austauschen.

Damit die Kommunikation auf der von allen Teilnehmern gemeinsam genutzten Funkfrequenz nicht unter Kollisionen zusammenbricht, kommt das Verfahren CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) zum Einsatz. CSMA/CA findet hauptsächlich in drahtlosen Netzwerken Verwendung und ist eine modifizierte Version des CSMA/CD-Zugriffsverfahrens, das in Kabelnetzen eingesetzt wird.

Das CSMA/CA-Verfahren ist in IEEE 802.11 standardisiert. Ähnlich wie bei CSMA/CD hören alle teilnehmenden Stationen den Verkehr auf dem Funkkanal mit. Bevor eine Station sendet, wartet sie, bis das Medium frei ist. Nach einer vorbestimmten Zeitperiode (DIFS) plus einer zufällig gewählten Zeitspanne beginnt die Station mit der Übertragung des Frames. Auch während dieser Zeitspanne (Wettbewerbsfenster) wird der Funkkanal überwacht. Hat aber eine andere Station innerhalb der Wartezeit mit der Übertragung begonnen, wird der Zeitzähler angehalten und nach der Übertragung der anderen Station weiterbenutzt. Auf diese Weise gewinnen Stationen, die nicht übertragen durften, an Priorität und kommen mit einer erhöhten Wahrscheinlichkeit in den nächsten Wettbewerbsfenstern zum Zug. Eine Kollision kann somit nur entstehen, wenn zwei oder mehrere Stationen dasselbe Zeitfenster auswählen. Diese Stationen müssen die Wettbewerbsprozedur erneut durchlaufen.

Ein Access Point ist für die Vergabe der Zeitfenster an die einzelnen Clients verantwortlich, in einem anderen Zeitfenster werden die Daten vom Access Point als Mittler an das Zielgerät weitergeleitet. Ebenso wie bei einem Switch, der im kabelgebundenen Ethernet die Netzwerkkarten mehrerer Endgeräte auf einen parallelen Datenbus schaltet, schafft ein Access Point einen funkbasierten Datenbus, über den die eingebuchten Endgeräte Daten austauschen können.

Zur Verbindung des W-LANs mit einem leitungsgebundenen Ethernet besitzt ein Access Point eine RJ-45-Buchse. Über diese Schnittstelle werden die Signale zwischen dem funkbasierenden und dem leitungsgebundenen Medium ausgetauscht. Weil diese Charakteristik einer Bridge entspricht, wird dieser Vorgang auch als „Bridging“ bezeichnet.

Hardware-Optionen: Funken auf allen Kanälen

Ältere Access Points arbeiteten ausschließlich nach dem IEEE-802.11b-Standard. Seit der Marktreife von 802.11g-Geräten sind diese erheblich preiswerter geworden. Wenn Sie in Ihrem drahtlosen Netzwerk ältere Geräte nach 802.11b verwenden und nur geringe Datenmengen über das Netzwerk schicken und wenn Ihre Breitband-Anbindung weniger als 3 MBit/s übertragen kann, bringt ein 802.11g-Access-Point keine Vorteile.

Wird das W-LAN dagegen sehr häufig und mit großen Datenmengen genutzt oder besitzen Sie bereits Netzwerkgeräte nach dem aktuellen Standard 802.11g, sollten Sie den finanziellen Mehraufwand nicht scheuen und einen 802.11g-Access-Point einsetzen. Weil diese Geräte rückwärtskompatibel sind, können ältere 802.11b-Geräte weiter genutzt werden.

Seit Ende 2002 ist in Europa auch der Standard IEEE 802.11a zugelassen, der im 5-GHz-Bereich genau wie 802.11g Datentransferraten von 54 MBit/s (brutto) bietet. Allerdings ist die Akzeptanz der 802.11a-Geräte – auch aus Kompatibilitätsgründen – sehr gering, was sich im Preis bemerkbar macht.

Antennen: Anschluss gesucht

Viele, aber noch längst nicht alle Access Points verfügen über einen zusätzlichen Antennen-Anschluss oder über die Möglichkeit, die eingebaute Dipol-Antenne gegen eine Hochleistungs-

KNOW-HOW

Wireless-LAN-Hardware in der Übersicht

Gerät	Verbindung	Funktion	Bemerkungen
Access Point (AP) oder Wireless Gateway	Internet-Verbindung, manchmal via LAN	Funktioniert wie ein Hub im Ethernet, sorgt für die gemeinsame Nutzung der Internet-Verbindung, verbindet drahtlose und leitungsgebundene Geräte.	Arbeitet oft nur unter Windows. Apple- und Unix-Nutzer gucken meist in die Röhre; es werden nur Windows- beziehungsweise IP-Protokolle unterstützt.
Drahtlose Netzwerkkarte (Funknetzwerkkarte)	Netzwerk-Computer	Verbindet Computer und andere Netzwerkgeräte drahtlos mit einem Access Point.	Benötigen eigene Treiber.
Antenne	Access Point oder Funknetzwerkkarte	Erweitert die Reichweite, meistens in das Gerät eingebaut.	Bringt oft keine Verbesserung.
Bridge (drahtlos)	LAN	Verbindet ein drahtloses mit einem leitungsgebundenen Netzwerk.	Manche Bridge verbindet nur mit einem Netzwerk, bessere Geräte können mehrere Netzwerke verbinden.
Relais (drahtlos)	W-LANs	Erweitert die Reichweite eines W-LANs durch Weiterleitung des Signals.	Datenrate oft reduziert, weil die Relais-Station die Pakete vom Sender und Empfänger weiterleiten muss.

BASISSTATION: Access Points wie der EtherFast von Linksys oder Apples AirPort funktionieren wie ein Hub im LAN.

EINGEBAUT: Funknetzwerkkarten wie diese W-LAN-Karte sind im PCI-Slot des Rechners untergebracht.

antenne auszutauschen. Durch den Einsatz einer leistungsfähigen Antenne lässt sich die Reichweite des drahtlosen Netzwerks beträchtlich steigern. Das ist besonders wichtig, wenn die Funksignale bis zu einem anderen Access Point oder in ein anderes Gebäude reichen sollen.

W-LAN-Antennen können im Innen- und Außenbereich eingesetzt werden. Für die unterschiedlichen Aufgaben bieten die Hersteller spezielle Antennentypen an. Möchten Sie den Sendebereich Ihres drahtlosen Netzwerks erweitern oder zusätzliche Access Points aufstellen, sollten Sie sich nur solche Access Points anschaffen, die Sie mit einer zusätzlichen Antenne ausrüsten können. Einen ausführlichen Beitrag zum Thema „Antennen fürs W-LAN“ lesen Sie ab **50**.

Ethernet-Anschluss: Problemlos ins Kabel-LAN

Ein Access Point verfügt über mindestens zwei Ethernet-Schnittstellen: eine für den WAN-Anschluss via Breitband-Modem und eine für die LAN-Verbindung zu einem Computer oder Hub. Die neueren Access Points unterstützen am WAN-Anschluss 100 MBit/s, auch wenn das viel mehr ist, als zum Beispiel für ein DSL-Anschluss (derzeit etwa 6 MBit/s) benötigt wird. Auf der LAN-Seite arbeitet der Access Point als Hub oder Switch. Unterstützt werden an dieser Stelle die Ethernet-Transferraten von 10/100 MBit/s. Ein Access Point stellt sich – wie auch alle modernen LAN-Switches – automatisch auf die Transferraten im Ethernet ein (Auto-Switching).

Modem: Es muss nicht immer DSL sein

Nicht jeder ist in der glücklichen Lage, einen Breitbandanschluss zum Internet zu besitzen. In diesem Fall müssen Sie auf ein analoges oder ein ISDN-Modem zurückgreifen. Nur sehr wenige Access Points verfügen über ein eingebautes Modem, die meisten lassen sich jedoch über eine serielle Schnittstelle mit einem analogen oder ISDN-Modem verbinden.

Betriebsmodi: Vielseitig verwendbar

Manche der 802.11-Basisstationen unterstützen verschiedene Betriebsmodi: Sie können also gleichzeitig Verbindungen zu anderen Access Points und Clients aufbauen. Bei den möglichen Betriebsmodi eines 802.11-Access-Points kann es sich handeln um:

Basic Service Set (BSS)
Extended Service Set (ESS)
Ethernet Bridge
Wireless Bridge
Wireless Repeater
Wireless Distributed System

Diese Betriebsarten werden auch als Infrastruktur-Modus bezeichnet. Im Gegensatz dazu kommuniziert im Ad-hoc-Modus eine Gruppe von Netzwerkgeräten direkt miteinander (Peer to Peer), ohne dass dabei ein Access Point zum Einsatz kommt.

Im Basic Service Set arbeitet ein einzelner Access Point, an dem sich beliebig viele Endgeräte einbuchen und Daten austauschen können. Unterstützt ein Access Point den Modus Ethernet Bridge, bietet er neben der Funkschnittstelle noch eine interne Netzwerkkarte mit RJ-45-Buchse als Schnittstelle in das kabelgebundene Ethernet und vermittelt die Daten zwischen Ethernet und Wireless LAN.

Für das Extended Service Set verbindet man zwei oder mehr Access Points über ein Ethernet und stellt den gleichen Funknetzwerknamen (SSID) ein. Dadurch vergrößert sich die Reichweite des Funknetzes, denn die Clients werden in der Folge automatisch zwischen den Access Points übergeben, sobald sich der Standort des Clients entsprechend geändert hat. Dieser Vorgang wird als Roaming bezeichnet.

W-LAN-Karten: Diese Typen gibt es

Im Gegensatz zum Access Point sind W-LAN-Karten meist im Gehäuse des Computers untergebracht. Sie stecken beim Desktop-PC in einem PCI-Slot, im Notebook im PC-Card-Schacht oder in einer anderen Schnittstelle. Ist innerhalb des Rechners kein Platz, lässt sich der W-LAN-Adapter auch in einer USB- oder in der Ethernet-Schnittstelle unterbringen.

Die beste Option ist die Montage innerhalb des Client-Computers, denn diese internen Karten sind nicht nur preiswerter, sondern auch gut vor Beschädigungen geschützt. Die Tabelle auf **49** gibt Ihnen einen Überblick über die am häufigsten verwendeten W-LAN-Karten.

PC Card: Slots für PC Cards befinden sich in jedem Notebook. Und weil Notebooks die idealen Geräte für ein drahtloses Netzwerk sind, gibt es diesen Kartentyp in ziemlich großer Auswahl. Wi-Fi-Karten besitzen eine eingebaute Antenne (Mini-Dipol). Der größte Unterschied liegt in der Sendeleistung der PC Cards. Es gibt Karten, die mit 30 Milliwatt senden, andere schaffen 100 oder 200 Milliwatt, was sich in der Reichweite deutlich bemerkbar macht. Interessant sind PC Cards für Windows- und Linux/Unix-Benutzer, moderne Apple-Macintosh-Rechner besitzen eine interne AirPort-Karte.

PCI-Karten: Alle PCs (ein paar Kompaktmodelle einmal ausgenommen) besitzen PCI-Steckplätze für Erweiterungskarten wie →

zum Beispiel Funknetzwerkkarten. Diese verfügen meistens über eine externe Antenne und/oder einen Anschluss für Hochleistungsantennen.

Mini-PCI-Karten: Zahlreiche Notebooks, die die Centrino Mobile Technology von Intel verwenden, besitzen Steckplätze für Mini-PCI-Karten. Der Vorteil: Diese Karten verbrauchen wenig Strom und arbeiten mit externen Antennen zusammen.

USB: Dieser Anschluss, häufig für Tastatur, Maus oder Drucker benutzt, kann auch einen externen W-LAN-Adapter aufnehmen. USB 1.1 arbeitet mit 12 MBit/s etwas schneller als der Standard IEEE 802.11b. USB 2.0 schafft 480 MBit/s, genug für die Standards 802.11a und g, die 54 MBit/s übertragen.

Ethernet-Karte: Ältere PCs, Xbox und Playstation besitzen häufig nur Ethernet-Ports für den Anschluss eines W-LANs. In diesen Fällen wird die W-LAN-Karte durch eine Wireless Ethernet Bridge direkt mit der Ethernet-Karte verbunden.

Compact Flash: Viele Handhelds, Organizer, Kameras oder MP3-Player unterstützen eine Wi-Fi-Compact-Flash-Karte zur Synchronisation der Daten oder zur Verbindung mit dem Internet. Die mobilen Helfer senden mit maximal 11 MBit/s, die WEP-Verschlüsselung (bis 128 Bit) wird unterstützt.

AirPort/AirPort Extreme: Durch diese internen Funknetzwerkkarten nach IEEE 802.11b können Apple-Rechner in einem W-LAN kommunizieren. 2003 wurde die AirPort-Karte durch AirPort Extreme (IEEE 802.11g) abgelöst. Ältere Macs arbeiten noch mit PC Cards oder PCI Cards.

In neueren Pocket PCs und Palm-Handhelds sind W-LAN-Karten bereits eingebaut. Zur Verbindung mit dem Rest der Welt arbeiten diese Karten meistens nach dem IEEE-802.11b-Standard, sie unterstützen Ad-hoc- (ohne Access Point) und Infrastructure-Netzwerke (mit Access Point).

Bridges: Netzwerke verbinden

Eine Brücke (engl. bridge) verbindet in einem Computernetzwerk zwei Segmente auf der Ebene der Schicht 2 (Sicherungsschicht) des OSI-Modells. Eine Bridge wird hauptsächlich

BLITZ-WORKSHOP

Access Point aufstellen und konfigurieren

Bevor Sie mit der Installation der Hardware beginnen, denken Sie daran, dass beim Setup eines Infrastructure-Netzwerks alle W-LAN-Geräte in den Infrastructure-Modus geschaltet werden. Entsprechendes gilt für ein Ad-hoc-Netz: Hier müssen alle W-LAN-Geräte im Ad-hoc-Modus arbeiten.

1 Suchen Sie den optimalen Aufstellpunkt für den Access Point. Der beste Platz ist in vielen Fällen im Mittelpunkt des W-LAN. Ideal ist, wenn sich keine störenden Hindernisse zwischen Access Point und W-LAN-Gerät befinden.

2 Richten Sie die Antenne so aus, dass sie das gesamte W-LAN abdeckt. In den meisten Fällen ist eine hohe Platzierung ideal. Eine gut arbeitende Antenne erhöht den Datendurchsatz spürbar.

3 Verbinden Sie in einem Infrastructure-Netzwerk das LAN-Kabel mit dem Access Point, das andere Ende mit dem Router oder Hub.

4 Access Points benötigen eine eigene Stromversorgung. Schließen Sie den Access Point an das Stromnetz an.

Nachdem der Access Point aufgestellt und mit dem LAN verbunden ist, geht es an die Einrichtung des Access Points. Das geschieht von einem beliebigen LAN-Computer aus, die Einstellungen sind aber auch über ein W-LAN-Gerät möglich. In den meisten Fällen hilft Ihnen ein Setup-Wizard bei der Aufgabe. Im folgenden Beispiel richten wir unter Windows XP einen Wireless Access Point von Linksys ein, andere Setups funktionieren ähnlich.

5 Schalten Sie den Access Point durch Drücken des Netzschalters ein.

6 Legen Sie die CD mit der Access-Point-Software in das CD-Laufwerk.

7 Nach dem Autostart der CD sehen Sie die Willkommens-Nachricht des Setup-Wizard auf dem Bildschirm. Klicken Sie auf „Setup“ und anschließend auf „Next“.

8 Zunächst wird Ihnen angezeigt, wie der Access Point mit dem übrigen Netzwerk verbunden ist. Lesen Sie die Informationen und klicken Sie auf „Next“.

9 Der Setup-Wizard durchsucht jetzt das gesamte W-LAN und zeigt Ihnen die Statusmeldungen aller gefunden Access Points. Ist nur ein Access Point vorhanden, wird nur dieser angezeigt. Klicken Sie auf „Next“.

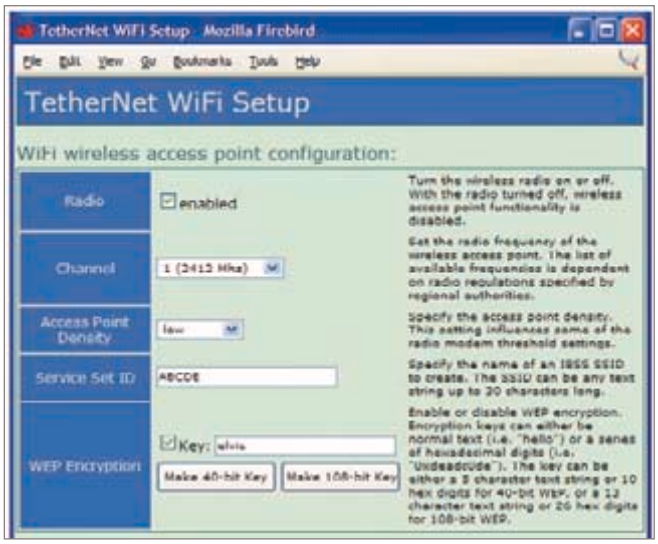
10 Geben Sie im nächsten Fenster das zugehörige Passwort zur Verwaltung des Access Point ein (Voreinstellung: admin). Klicken Sie zum Schluss auf „OK“.

11 Im nächsten Fenster geht es um die Netzwerk-Einstellungen. Geben Sie die IP-Adresse, Subnetzmaske und IP-Adresse des Gateways ein. Klicken Sie dann erneut auf „Next“.

12 Weiter geht's. Jetzt folgt die Eingabe von SSID und des Kanals, auf dem das Netzwerk sendet. Meist ist noch ein Gerätename einzugeben. Klicken Sie dann wieder auf „Next“.

13 Ein Fenster mit den Sicherheitseinstellungen erscheint. Legen Sie fest, welcher Sicherheitslevel bei der Verschlüsselung der Signale in Ihrem W-LAN gelten soll. Meistens bieten die Hersteller mehrere Optionen an. Die gleichen Einstellungen müssen auf allen Netzwerkgeräten vorhanden sein. Klicken Sie anschließend erneut auf „Next“.

14 An dieser Stelle ist die Konfiguration des Access Points abgeschlossen. Klicken Sie im letzten Fenster des Setup-Wizards auf „Exit“.



EINSTELLUNGSSACHE: Beim Konfigurieren des Access Points sollten Sie sich für die stärkste Verschlüsselung entscheiden – in diesem Fall für eine Schlüssellänge von 108 Bit.

KNOW-HOW

Die am häufigsten verwendeten W-LAN-Adapter

Gerät	PC Card	PCI Card	Mini PCI Card	USB	Ethernet-Adapter	Compact Flash	AirPort/AirPort Extreme	Eingebaut
Desktop-PC	–	●	–	●	●	–	–	–
Notebook	●	–	●	●	●	–	–	–
iBook/iMac	–	–	–	●	●	–	●	–
Power Mac (ab 2003)	–	●	–	●	●	–	●	–
Pocket PC	●	–	–	–	–	●	–	●
Palm Handheld	–	–	–	–	–	–	–	●

benutzt, um ein Netz in verschiedene Kollisionsdomänen aufzuteilen. Dadurch wird besonders in großen Netzwerken die Last vermindert, da jeder Netzstrang nur die Pakete empfängt, deren Empfänger sich auch in diesem Segment befindet. In der Netzwerktechnik wird dabei zwischen einer MAC-Bridge und einer LLC-Bridge unterschieden. Eine weitere Unterscheidung ergibt sich durch die Art der Leitwegermittlung von Datenpaketen in Transparent Bridge und Source Routing Bridge.

Eine MAC-Bridge verbindet Netze mit gleichen Zugriffsverfahren. Die LLC-Bridge (auch Remote-Bridge oder Translation Bridge genannt) wird verwendet, um zwei Teilnetze mit verschiedenen Zugriffsverfahren (etwa CSMA/CD und Token-Passing) zu koppeln. Innerhalb der LLC-Bridge findet eine Umsetzung (Translation) statt. Bei dieser Umsetzung werden alle Parameter des Quellnetzes, beispielsweise MAC-Adresse, Größe und Aufbau des MAC-Frames, an das Zielnetz angepasst.

Im täglichen Betrieb lernt eine Transparent Bridge, welche MAC-Adressen sich in welchem Teilnetz befinden. Die Empfänger und Absender von Paketen in den einzelnen Teilnetzen werden in eine interne Weiterleitungstabelle eingetragen. Anhand dieser Informationen kann die Bridge den Weg zum Empfänger bestimmen. Die Absenderadressen werden laufend aktualisiert, um Änderungen sofort zu erkennen. Eine Source Routing Bridge besitzt keine Weiterleitungstabelle. An dieser Stelle muss der Sender die Informationen zur Weiterleitung zum Ziel bereitstellen.

Ist der Empfänger nicht in der Weiterleitungstabelle eingetragen, wird ein Paket in alle Teilnetze gesendet (Broadcast). Nur im ungelernten Zustand wird jeder eingehende Frame an alle Ports im Netzwerk gesendet (außer an den, der den Frame gesendet hat). Beim Durchgang durch eine Bridge werden sämtliche Paket-Frames überprüft und nur korrekte Frames werden weitergereicht.

Gateway: Das Tor zur Welt

Als Gateway (deutsch: „Einfahrt, Durchgang“) bezeichnet man einen Übergang zwischen Netzwerken mit verschiedenen Protokollen. Gateways gibt es wiederum als Hardware- oder Softwarelösung. Das Gerät oder Programm konvertiert die Daten des Senders in ein Format, das von den Protokollen des empfangenden Netzes unterstützt wird.

Ein Internet-Gateway ist ein Gerät, das die Verbindung zwischen der Hauptdatenleitung (Backbone) und einem daran angeschlossenen anderen Netz, beispielsweise einem LAN, ermöglicht. Ein Gateway führt in der Regel die Protokoll-Konvertierung zwischen dem Backbone und dem Sub-Netz aus, wandelt die Daten um und übermittelt Nachrichten.

Backbones bestehen oft aus eigenständig arbeitenden Hochgeschwindigkeits-Netzen, bei denen die Daten durch Glasfaserkabel übertragen werden. Bevor diese Daten in das aus Kupferkabeln bestehende Telefonnetz eingespeist werden können, müssen sie von optischen Signalen (Lichtimpulsen) in elektrische Ströme umgewandelt werden. Ein Gateway kann eine Verbindung zwischen einem auf dem Internet-Protokoll (TCP/IP) beruhenden lokalen Computernetz und einem weiteren Netzwerk herstellen, das auf einem proprietären Netzwerkprotokoll, beispielsweise auf dem von der Firma Apple stammenden Appletalk, beruht.

Router: Der Verbindungsrechner

Ein Router ist ein Vermittlungsrechner, der in einem Netzwerk dafür sorgt, dass bei ihm eintreffende Daten eines Netzwerks zum vorgesehenen Zielnetz weitergeleitet werden. Router arbeiten auf Schicht 3 (der Netzwerkebene) des OSI-Referenzmodells. Ein Router ist somit im Gegensatz zu einer Bridge nicht auf ein bestimmtes Übertragungsmedium beschränkt, sondern kann Medien unterschiedlicher Netzwerke miteinander verbinden.

Für jedes angeschlossene Netzwerk besitzt ein Router eine Schnittstelle. Beim Eintreffen von Daten muss das Gerät den richtigen Weg zum Ziel und damit die passende Schnittstelle, über die die Daten weiterzuleiten sind, bestimmen. Dazu bedient er sich einer lokal vorhandenen Routing-Tabelle. Die Einträge in dieser Tabelle können statisch oder dynamisch sein. Statische Einträge werden durch die Einträge eines Netzwerk-Administrators erzeugt. Dynamische Einträge resultieren aus Routing-Protokollen.

Wer sich keinen Hardware-Router anschaffen will, kann auch seinen Computer mit entsprechenden Programmen zum Router machen. Auf einem Windows-PC gibt es etwa seit Windows 98 die Möglichkeit, einen Software-Router namens Internetverbindungsfreigabe für das Netzwerk bereitzustellen.

Peter Klau

Weiter funken

Die richtige Antenne kaufen

In Access Points und W-LAN-Karten sind die Antennen bereits eingebaut. Bedingt durch ihre Bauform und Größe haben sie allerdings nur eine begrenzte Reichweite. Um weiter funken zu können, sind Sie mit einer externen Antenne oft besser bedient. CHIP sagt Ihnen, worauf Sie bei der Wahl der Antenne achten müssen.

Die Antenne ist eine sehr wichtige Komponente eines W-LAN. Die Antenne des Senders sendet Hochfrequenzenergie aus, während die Antenne des Empfängers diese auffängt und in Elektrizität umwandelt. Im einfachsten Fall erhöht eine Antenne die Sende- und Empfangsleistung eines Transceivers (Kombination aus Transmitter und Receiver), der Antennengewinn kommt durch eine Richtwirkung der Antenne zustande.

Gerichtet und ungerichtet

Es gibt zwei Kategorien – die Richtfunk- und Sektor-Antennen, die man auch als direktionale und omnidirektionale Antennen bezeichnet. Eine onmidirektionale Antenne (auch Rundstrahlantenne) setzt man zur Verbreitung von Radiowellen ein, weil sie in alle Richtungen abstrahlt. So verfügt jedes Handy oder Polizei- und Feuerwehrfahrzeug über eingebaute omnidirektionale Antennen. Auch in jede W-LAN-Karte in einem PC ist eine in alle Richtungen sendende Antenne eingebaut.

Die klassische Ausführung einer Rundstrahlantenne ist der Halbwellendipol. Dabei ist die Antennenlänge gleich der halben Wellenlänge. Horizontal hat diese Antenne eine Rundstrahlcharakteristik, vertikal einen Abstrahlwinkel von 78 Grad.

Die direktionale Antenne, auch Richt- oder Sektor-Antenne genannt, strahlt ihre Energie hauptsächlich in eine Richtung ab. Auch sie gibt es für alle Zwecke und Anforderungen, mit kleinerem Abstrahlwinkel oder großem. Direktionale Antennen fürs W-LAN sind etwa die Yagi- und die Parabol-Antenne.

Eine Yagi-Antenne besteht meist aus einem Dipol und einem Reflektor, der in eine oder mehrere Richtungen abstrahlt. In der Regel ist die Yagi-Antenne in einem Kunststoffzylinder untergebracht, der sie vor Wettereinflüssen und Feuchtigkeit schützt. Yagi-Antennen sind klein, aber effektiv und preiswert. Oft strahlen sie in zwei oder mehr Richtungen ab und können Funkkontakt mit zwei unterschiedlichen Access Points aufnehmen.

Eine Parabol-Antenne empfiehlt sich, wenn es darum geht, das Antennensignal zu bündeln, um damit einen bestimmten Bereich abzudecken.

Alle Antennen besitzen ein bestimmtes Abstrahlmuster (Charakteristik) und konzentrieren ihre Energie – mit Ausnahme der omnidirektionalen Antenne – auf eine bestimmte Richtung. Die größte Energiekonzentration findet sich in der Antennenachse. Der Abstrahlwinkel direktionaler Antennen variiert von 270 bis 0,5 Grad. Die gebräuchlichsten Antennen für ein W-LAN bieten 5 bis 45 Grad, Yagi-Antennen mit Mehrfachelementen offerieren 15 bis 20 Grad. Bei Parabol-Antennen können Sie mit einem Winkel von 5 bis 10 Grad rechnen.

DIE WICHTIGSTEN ANTENNENARTEN

Antennenart	Verwendung
Peitschen- oder Stabantenne	Ungerichtete Antennen für Mobiltelefone sowie W-LAN- und ähnliche Geräte
Dipol-Antenne	Verwendung hauptsächlich im Amateurfunk
Yagi-Uda-Array	Typische Fernsehantenne: Dipol-Antenne mit starker Richtwirkung, muss in Richtung des Senders positioniert werden
Parabol-Antennen	Zum Empfang von Satellitensignalen, sehr starke Richtwirkung, müssen sehr genau ausgerichtet werden

Antennengewinn

Die Leistung von Antennen misst man in Dezibel (dB). Unter Antennengewinn versteht man, wieviel Leistung eine Testantenne bezogen auf eine standardisierte Referenzantenne bei gleicher Eingangsleistung abgibt. Der Gewinn einer Antenne entsteht durch die Bündelung des Signals (Richtwirkung). Richtfunk-Antennen strahlen gezielt in eine Richtung, haben einen sehr kleinen Öffnungswinkel, also einen hohen Gewinn. Bei gleicher Sendeleistung lässt sich so mit einer Richtantenne eine viel weitere Strecke überbrücken.

Zur Angabe des Antennengewinns gibt es zwei Methoden. Bei der ersten wird eine isotrope Antenne als Referenz verwendet, bei der zweiten eine andere Art von Antenne (gewöhnlich eine Halbwellendipolantenne).

Bei Verwendung einer isotropen Antenne als Referenz wird der Gewinn „absoluter Gewinn“ genannt und in der Einheit dBi (Dezibel über Isotopenstrahler) angegeben.

Bei Verwendung eines idealen Halbwellendipols als Referenz wird der Gewinn „relativer Gewinn“ genannt und in der Einheit dBd (Dezibel über Dipol) angegeben.

Ein Beispiel für die Angabe eines Antennengewinns: eine Antenne hat einen Gewinn von 3 dBd. Die Ausgangsleistung des Funkgeräts sei 0,5 Watt. 3 dB entsprechen der rund zweifachen Leistungssteigerung. Die Antenne strahlt jetzt aber nicht mit 1 Watt (2 x 0,5), sondern die Gegenstation empfängt gleich laut, als ob sie mit einem Dipol und 1 Watt senden würde.

Vorschriften und Gesetze

Um einen möglichst reibungslosen Betrieb der Geräte mit- und nebeneinander zu gewährleisten, gibt es eine Reihe von Gesetzen und Vorschriften. Laut Regulierungsbehörde für Telekommuni-

Die besten Antennen-Tipps im Web

WiMo Antennen GmbH → www.wimo.de
Alle Arten von Antennen für professionelle Anwendungen
Oelschläger Elektronik GmbH
→ www.steckerprofi-shop.com
Antennen, W-LAN-Flat Patch, W-LAN-Rundstrahler, W-LAN-Yagis
Meconet → www.wireless-lans.de
Spezialisiert auf den Einsatz von W-LAN im Außenbereich. Qualifiziertes Know-how, Lösungen und Zubehör

kation und Post (**www.regtp.de**) darf in der Europäischen Union eine Sendeleistung von 20dB nicht überschritten werden. Die Sendeleistung setzt sich zusammen aus der Leistung des W-LAN-Geräts abzüglich aller Verluste (Dämpfung) in Adaptern oder Kabeln zuzüglich des Antennengewinns. Wenn Sie etwa einen Access Point mit 20 dB Ausgangsleistung an ein Antennenkabel mit einer Dämpfung von 3 db anschließen, verbleiben am Ende des Kabels 20 dB - 3 dB = 17 dB. Um die zulässigen 20 dB nicht zu überschreiten, darf der Gewinn der Antenne höchstens 3 dB betragen. Das soll verhindern, dass sich einzelne W-LANs gegenseitig stören.

Wer gewerbliche Telekommunikationsdienstleistungen für die Öffentlichkeit erbringt, muss dies der Regulierungsbehörde schriftlich anzeigen. Wer aber einen oder mehrere Hotspots betreibt, um etwa ein Dorf mit W-LAN zu versorgen, muss das nicht genehmigen lassen, auch wenn zur Kostendeckung ein bestimmter Betrag dafür erhoben wird.

Antennen richtig montieren

Für die erfolgreiche Funkvernetzung ist die richtige Auswahl, Installation und Ausrichtung der Antennen die wichtigste Voraussetzung. Auch bei der Überbrückung geringer Entfernungen kann die Verbindung bei fehlerhafter Antenneninstallation unzuverlässig oder auch gar nicht funktionieren.

Ein wichtiger Punkt, der oft übersehen wird, ist die geringe vertikale Abstrahlung vieler Antennen, die meist im Bereich um die 10 Grad liegt. Auf kurze Entfernungen ist es daher ohne Kippen der Antennen sogar oft nicht möglich, auch nur ein Stockwerk problemlos zu überbrücken. Die Idee, einen hohen, zentralen Punkt mit einer Rundstrahlantenne zu versehen und dann Clients in der Umgebung mit einer Richtfunkantenne auf diesen Punkt auszurichten, funktioniert meistens nicht, da alle niedrigeren Punkte auch bei freier Sicht im Funkschatten der Rundstrahlantenne liegen. An dieser Stelle sind Sektor-Antennen eine professionelle Lösung, da diese in den Sektor gekippt werden können.

Bei der Installation insbesondere von Rundstrahlantennen ist darauf zu achten, dass sich auch in der Umgebung der Antennen möglichst wenige Hindernisse befinden. Die Weiterleitung der Funkwellen wird oft auch durch Hindernisse unter der Antenne beziehungsweise in Bereichen, die nicht versorgt werden sollen behindert (Fresnel-Zone). So sollten Sie eine Omni-Antenne nicht direkt auf einem Flachdach oder an einer Mauer befestigen. Optimal ist die Installation an einem (wenn auch kurzen) Mast (lesen Sie dazu auch den Beitrag über Wireless Bridges ab 110).

Bei der Überbrückung größerer Entfernungen insbesondere mit Richtfunkantennen oder beim Aufbau eines Sektorkreises empfiehlt sich auf jeden Fall die Zusammenarbeit mit professionellen Antennenbauern, die entsprechende Erfahrungen und auch Messgeräte haben. Die Einrichtung einer Richtfunkstrecke mit zwei Yagi-Antennen kann ansonsten auch auf kurzen Entfernungen schon problematisch sein.

Peter Klau

KNOW-HOW

W-LAN versus Umwelt

Es gibt eine Menge Faktoren, die den Empfang in einem Funknetzwerk nachhaltig stören können. Zu diesen gehören:

- **Mikrowellengeräte**
- **TV-Geräte**
- **Heizkörper (Fußbodenheizung!)**
- **Metallflächen**
- **Fenster, Jalousien**
- **Elektrogeräte, Babyphone**
- **Elektrische Garagentore**
- **Decken und Wände**
- **Bäume**
- **Simultaner Betrieb anderer Funknetze (Bluetooth) in der Nachbarschaft**

Praxis-Tipp: Vor der Anschaffung des Funk-LAN-Equipments leihen Sie sich von einem Bekannten oder Fachhändler die Geräte und testen zunächst einmal die Empfangseigenschaften für das Funknetz.

PROFI-TIPPS

W-LAN-Antenne richtig installieren

Nicht nur auf Gewinn achten Die beste Antenne ist nicht zwangsläufig die mit dem größten Gewinn. Antennen vergrößern den Gewinn durch Konzentration der Radiowellen. Eine Antenne mit großem Gewinn bündelt die Signale sehr stark. Für die Abdeckung einer großen Fläche ist eine omnidirektionale Antenne besser.

Signalstärke messen Bevor Sie einen Access Point aufstellen, messen Sie die Signalstärke. Oft reichen ein paar Meter, um ein besseres Signal zu bekommen.

Idealposition testen Positionieren Sie ein Notebook zunächst im Ad-hoc-Modus an einem Arbeitsplatz, um zu sehen, ob ein Empfang möglich ist.

Kritische Ecken checken Bevor Sie die Installation einer Antenne abschließen, messen Sie die Signalstärke an allen problematischen Orten. Jeder Antennentyp hat seine spezielle Abstrahlcharakteristik, manchmal reicht es, die Antenne etwas zu drehen.

Kurzes Kabel nehmen Je länger das Kabel vom Access Point zur Antenne, desto größer der Signalverlust. Verwenden Sie ein möglichst kurzes Kabel und mit extrem niedriger Dämpfung.

Sendeleistung testen Achten Sie darauf, dass die Sendeleistung Ihrer W-LAN-Geräte nahe am zulässigen Maximum von 20 dB liegt. Es gibt auch preiswerte Geräte, die lediglich 14 dB schaffen. Die sind nur für unproblematische, kurze Verbindungen geeignet.

Empfangsempfindlichkeit Auch sie ist wichtig. Gute Geräte erreichen Werte bis zu -97 dB. Je höher der Zahlenwert ist , um so schwächere Signale kann das Gerät noch empfangen.

W-LAN perfekt einrichten

Kabelloses Heimnetz

Mit Ihrem Funknetzwerk können Sie viel mehr als nur im Garten surfen. CHIP zeigt, was Ihnen die vielfältigen Einsatzmöglichkeiten bieten, und hilft Ihnen, Stolperfallen bei der Einrichtung zu vermeiden. Zusätzlich bieten wir noch Experten-Tipps und zeigen, wie Sie nicht W-LAN-fähige Geräte ins Netz einbinden.

Keine störenden Kabel mehr, Internet überall, Videos mit digitalem Ton im Wohnzimmer – drahtlose W-LAN-Netze versprechen Internet und Multimedia im ganzen Haus und das ohne aufwendige Verkabelung. Doch damit Sie die neue kabellose Welt nutzen können, müssen Sie die entsprechenden Komponenten erst einmal installieren und konfigurieren; aber das ist manchmal gar nicht so einfach. Die Hersteller versprechen große Reichweiten und eine einfache Einrichtung mit ein paar Mausklicks, die Realität sieht allerdings anders aus: es gilt störende Funkhindernisse zu umgehen, Verschlüsselungsmethoden richtig zu wählen und andere Komponenten perfekt in das Netz einzubinden. CHIP zeigt, wie Sie die W-LAN-Stolperfallen umgehen können und in ein paar einfachen Schritten zum perfekten W-LAN kommen, das auch noch sicher ist. Wir erklären außerdem wo der beste Platz für Ihren Access-Point (AP) ist und wie Sie nicht W-LAN-fähige Geräte ans kabellose Netz anschließen können.

1 | Der richtige Funkstandard für Ihr Netz

Die Funkstandards für W-LAN spezifiziert der Industrieverband IEEE (Institute of Electrical and Electronical Engineers). Den Anfang machte in Deutschland der Standard IEEE 802.11b: Theoretisch 11 MBit/s schnell, lassen sich damit in der Praxis unter günstigen Bedingungen Datenübertragungsraten von 2 bis 5 MBit/s (entspricht etwa 0,5 MByte/s) erzielen. Das reicht gerade noch zum drahtlosen Internet-Surfen oder zum Abspielen von MP3-Dateien. Inzwischen sind aber fast nur noch W-LAN Router nach dem schnellen 802.11g-Standard erhältlich, die offiziell Raten von 54 MBit/s versprechen – in der Realität aber etwa 20 MBit/s (entspricht rund 2,5 MByte/s) erreichen. Damit lassen sich bereits Filme in voller DVD-Qualität übertragen. Zum Vergleich: Das kabelgebundene Fast Ethernet mit 100 MBit/s erreicht in der Praxis zirka 64 MBit/s, also 8 MByte/s.

Sowohl b- als auch g-Geräte funken in einem Frequenzband zwischen 2,4 und 2,5 GHz, einem Bereich mit sehr speziellen Eigenschaften: Wasserhaltiges Material jeder Art nimmt hier ein Maximum an Energie auf und raubt den elektromagnetischen Wellen ihre Energie. Mikrowellen, die meist mit einer Frequenz von 2,45 GHz arbeiten, nutzen diesen Effekt zum Erwärmen von Speisen. Für die Funkwellen eines W-LAN-Routers werden jedoch feuchte Wände, etwa Gips-Bauten zu undurchdringlichen Barrieren. Hinzukommt, dass in Deutschland, wie in den meisten anderen Ländern, die Sendeleistung für b/g-W-LAN auf maximal 100 Milliwatt begrenzt ist – Handys und DECT-Telefone senden dagegen mit bis zu 2 Watt. Immerhin stehen 13 Kanäle zur Verfügung – Teilbänder des Bereichs zwischen 2,4 und 2,5 GHz. Viele Kanäle sind gut für die Reichweite, weil die Geräte bei Störungen im gerade verwendeten Kanal auf einen anderen ausweichen können. Zum Vergleich: In den USA stehen nur elf Kanäle offen, in Frankreich gar nur acht. Der nominell 54 MBit/s schnelle 802.11a-Standard als dritter im Bunde arbeitet im 5-GHz-Band und handelt sich damit Probleme ganz anderer Art ein: In diesem Bereich funken nämlich Militär, Rettungsdienste, Polizei und Flugsicherung. Deshalb konnte sich der a-Standard in Deutschland nicht durchsetzen.

2 | Grundausstattung: DSL oder ISDN

Der Einstieg in die kabellose Freiheit beginnt mit einem Access Point und einer Funknetzwerk-Karte, die mindestens einen gemeinsamen Funkstandard unterstützen. Oft enthält der Access Point – die Funkzentrale, über die jedes teilnehmende Gerät kommuniziert – auch einen Router, der eine einfache Netzwerk-Struktur errichtet und mit einer Firewall dieses Netzwerk schützt. In der Regel verfügen solche Router über einen inte-

1 | KOMPLETTGERÄT: Der Access Point WL500g von Asus kann nicht nur als Router für Ihr Funknetz dienen, sondern zusätzlich noch Drucker über das W-LAN freigeben.

CHIP → DVD-CODE W-LAN

- → **WEP-Schlüssel testen** Mit den Gratis-Tools WEPCrack und AirSnort testen Sie, ob Ihre WEP-Schlüssel sicher gewählt sind und wie lange es dauert, diese zu knacken.
- → **W-LANs finden** Nutzen Sie den Network Stumbler, um offene und versteckte Wireless-Netze aufzuspüren oder den optimalen Standort für Ihren Access Point zu finden.

Die besten Adressen zum Thema W-LAN

IEEE-Komitee → www.ieee.org
Homepage der Zertifizierungsstelle des W-LAN-Standards
W-LAN Infos → www.informationsarchiv.net/statisch/wlan/
Alle wichtiges Infos über W-LAN kurz zusammengefasst
Hot-Spot-Verzeichnis → http://mobileaccess.de/wlan/
Hier finden Sie eine Liste kostenloser Internet-Hot-Spots
W-LAN Diskussionsforum → www.wireless-forum.ch/
Ein unabhängiges Diskussionsforum rund um W-LAN

grierten Switch mit Ethernet-Anschlüssen. Der Switch leitet den Datenverkehr immer nur genau dem PC zu, für den diese Daten bestimmt sind. Die meisten W-LAN-Router sorgen für den Internet-Zugang via DSL und beherrschen daher die Protokolle PPPoE (Point-to-Point-Protocol over Ethernet) und PPTP (Point-to-Point Transfer Protocol). Die Kombination aus AP und DSL-Router ist inzwischen ausgesprochen preiswert geworden: Für rund 65 Euro bekommen Sie schon einen komplett ausgerüsteteten Router mit Firewall-Eigenschaften und Druckserver, etwa den ASUS WL500g; gängige PC-Cards und PCI-Karten – die Gegenstellen im Funkverkehr – sind ab 50 Euro zu haben.

Für diejenigen, die lieber ISDN per W-LAN nutzen wollen, gibt es Lösungen ab 50 Euro und mehr: Die hier verwendeten speziellen Router müssen wenigstens einen seriellen Anschluss für einen ISDN-Terminaladapter oder ein Analog-Modem besitzen. Statt Kombigeräte zu verwenden wie bei einem DSL-Zugang bietet sich eher der Einsatz eines einfachen Routers und eines zusätzlichen W-LAN-Access-Points an. Vorteil: Der Access Point lässt sich funkgünstig aufstellen, während der Router in Modemnähe bleiben kann.

3 | So richten Sie den Access Point richtig ein

Nun müssen Sie Ihren neuen Router noch mit dem Netzwerk bekannt machen. Wie das funktioniert, erklären wir am Beispiel des Netgear WGR614. Für alle anderen Geräte gehen Sie analog vor, einzig die Menüpunkte heißen ein klein wenig anders. Falls Sie ein Netzwerkkabel haben, sollten Sie Ihren W-LAN-Router für die erste Konfiguration an die Netzwerkleine nehmen. Das ist erstens bequemer und es gehen zweitens keine ungesicherten Funkdaten bei der Konfiguration heraus. So nehmen Sie den Router in Betrieb: Schalten Sie den W-LAN-Router ein und danach Ihren Computer. Der Grund für diese Reihenfolge: Der Router ist in der Regel auch der DHCP-Server (Dynamic Host Configuration Protocol) in Ihrem Netzwerk. Startet der PC nach dem Router, dann erhält er automatisch eine IP-Adresse.

Verbinden Sie den Router mit Ihrem DSL-Anschluss und den einzelnen Rechnern. Öffnen Sie dann an einem beliebigen PC den Internet Explorer und tippen Sie „192.168.0.1“ in die URL. Klicken Sie nun auf den Punkt „Setup Wizard“; folgen Sie den Anweisungen. Damit sind die Grundeinstellungen vorgenommen. Ändern Sie als nächstes das Admin-Kennwort, denn Listen mit diesen Standard-Passwörtern findet jeder angehende Hacker im Web. Meist steht die entsprechende Option unter „Administration | Admin-Settings“ oder in der „Basiskonfiguration“. Achtung: Mit dem Zugriffskennwort sichern Sie nur den Router vor Manipulationen, nicht aber die Funkverbindung. →

KNOW-HOW

Access Point richtig aufstellen

Die Hersteller versprechen viel: Reichweiten über 100 Meter sollen kein Problem sein. Die Realität sieht aber meist anders aus. In manchen Fällen ist die W-LAN-Freude schon nach zehn Metern zu Ende. Grund dafür ist in vielen Fällen die Bauart des Gebäudes, in dem der Access Point steht. Aber auch die Ausrichtnug der Antenne und die Kompatibilität der einzelnen Wireless-Geräte sind wichtig.

Abstand zu Hindernissen Der Router/Access Point sollte nicht in unmittelbarer Nähe zu Versorgungsschächten oder -strängen aufgestellt werden. Je näher die Antenne am abschirmenden Hindernis steht, desto größer ist der Öffnungswinkel der dahinter entstehenden Abschattung. Wer eher eine horizontale Ausrichtung braucht – etwa für eine Wohnung –, stellt die Antenne besser senkrecht. Wer dagegen ein mehrstöckiges Reihenhaus versorgen will, wird in der Regel mit waagerechter Antenne bessere Ergebnisse erzielen. Bei der launischen Hochfrequenz-Übertragung hilft es übrigens manchmal schon, das Gerät um wenige Zentimeter zu verschieben. Einfaches Ausprobieren ist oft die beste Methode. Übrigens: An glatten Flächen wird das Signal teilweise reflektiert und gestreut, so stört ein Baum mit großen Blättern mehr als einer mit kleinen Blättern.

Nur ein Hersteller Beim Kauf eines W-LAN-Routers sollten Sie darauf achten, dass Sie Geräte des selben Herstellers kaufen. So stellen Sie sicher, das die Komponenten optimal aufeinander abgestimmt sind. Welche Hardware für Sie am besten geeignet ist, lesen Sie im Beitrag ab 44 in diesem Heft. Wenn die Räumlichkeiten sich nicht optimal auf den Access Point anpassen lassen, sollten Sie die Antenne möglichst hoch im Zimmer anbringen.

MIMO-Technologie Zusätzliche Hilfe bietet die neue MIMO-Technologie (Multiple Input, Multiple Output). Als erste setzte die Firma Netgear diese Technologie ein und nannte sie RangeMax. In den Geräten befinden sich sieben intelligente Antennen, mit denen 127 verschiedene Antennenmuster nachgebildet werden können. Diese ermöglichen die Anpassung an die jeweilige Netzwerkumgebung, indem sie sich an RF-Störungen (Radio Frequency), Positionen der Clients und physikalische Hindernisse anpassen. Mit der MIMO-Technologie lassen sich große Reichweiten sowie unterbrechungsfreie Datenübertragungsgeschwindigkeiten im Bereich des Funknetzwerks erzielen. Die MIMO-Komponenten kosten um die 100 Euro (mehr Infos finden Sie unter www.netgear.de).

REICHWEITEN-MESSUNG: Für die Messung der W-LAN-Reichweite gibt es teure Geräte. Wer nicht mehrere hundert Euro ausgeben will, nimmt das kostenlose Tool von Windows.

Gehen Sie dann auf die Netgear-Website **www.netgear.com** und laden Sie von dort die neueste Firmware für den Router herunter. Installieren Sie die Firmware über den Menüpunkt „Router Upgrade“. Damit ist das Gerät auf den neuesten Stand. Als nächstes erfolgt die Wireless-LAN-Einstellung und die Absicherung mit einer Verschlüsselungsmethode.

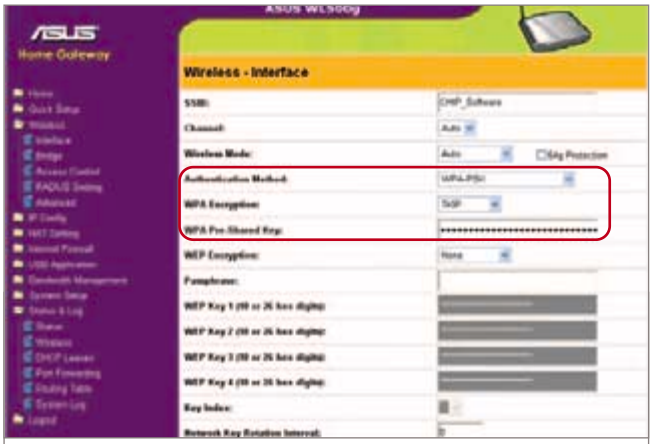
4 | Funksignale verschlüsseln

Nachdem Sie den Router selbst eingerichtet haben, geht es an das eigentliche Funknetz und dessen Verschlüsselung (mehr zum Thema Sicherheit lesen Sie im Special ab 68). Der gängigste Weg, ein Funknetz abzusichern, ist die Verschlüsselung der zu übertragenden Daten. Außenstehende bekommen so nichts mit vom Funkverkehr und können sich ohne Kennwort nicht einklinken. Der aktuell verbreitete Verschlüsselungsstandard WEP (Wired Equivalent Privacy), der in den meisten Funknetzen eingesetzt wird, weist allerdings Schwachstellen auf. Ein per WEP übertragenes Datenpaket setzt sich zusammen aus einem so genannten Initialisierungsvektor (IV) und den verschlüsselten Daten. Diese enthalten ihrerseits noch eine Check-Summe, um Manipulationen an den Daten selbst zu entdecken. Hauptschwachpunkt von WEP ist der Initialisierungsvektor. Er ist immer 24 Bit lang. Aus dem IV und dem WEP-Schlüssel errechnet ein Algorithmus den verschlüsselten Code.Und der wird dann per Funk übertragen. Aus dem dabei im Original übertragenen IV und dem WEP-Schlüssel ermittelt die Gegenstelle wieder die Original-Daten.

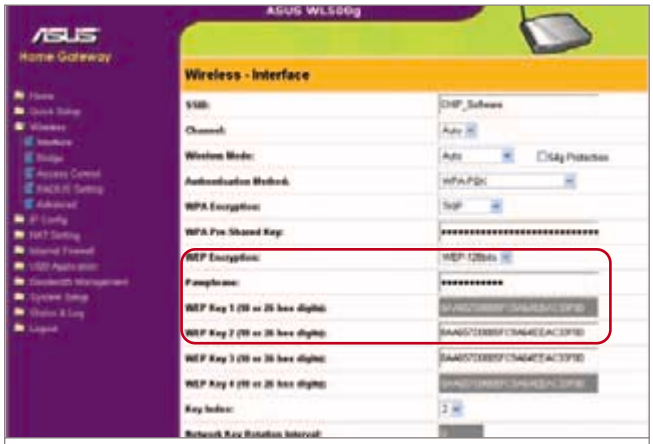
Das Problem: Zwar empfiehlt der WEP-Standard, dass jedes übertragene Paket einen anderen Initialisierungsvektor haben sollte. Aber erstens hält sich nicht jeder Hersteller daran und zweitens steht nirgends, wie der IV erzeugt wird. Meist wird ein Pseudo-Zufallsgenerator genutzt. Die Folge: Früher oder später wiederholt sich der IV. Ein Papier des Bundesamts für Sicherheit in der Informationstechnik rechnet damit, dass nach etwa 4.000 versandten Datenpaketen ein identischer IV auftaucht, die Universität von Berkeley spricht von 5.000 Paketen. Fängt ein Hacker zwei Datenpakete mit identischem Initialisierungsvektor ab, kann er daraus den WEP-Schlüssel ermitteln. Und schon haben Sie einen ungebetenen Gast im Netzwerk. Der kann Daten mitschneiden, sich beim Access Provider anmelden oder sogar Check-Summen fälschen und damit Daten manipulieren. Dafür braucht ein Angreifer nicht einmal teure Software. Programme, die WEP knacken, gibt es kostenlos im Internet etwa unter **http://wepcrack.sourceforge.net** oder **http://airsnort.shmoo.com.** Besonders einfach haben es Angreifer, wenn für die Verschlüsselung nur 40 Bit lange Schlüssel verwendet werden (64 Bit minus 24 Bit IV). Denn die sind so kurz, dass man die möglichen Kombinationen einfach durchprobieren kann und innerhalb kurzer Zeit den Code geknackt hat. Da die Schlüssel meist nur sehr selten gewechselt werden, lohnt dieser Aufwand für Angreifer. Danach steht das Funknetz für lange Zeit offen. Falls Sie also WEP nutzen, schalten Sie zumindest die Verschlüsselung mit 104 Bit ein (128 Bit minus 24 Bit IV). Das ist für Sie nur ein Mausklick – es verlängert die Rechenzeit für den Hacker jedoch ganz dramatisch.

Der neue Sicherheitsstandard WPA sperrt Hacker wirksam von Funknetzen aus. Wir zeigen, wie Sie Ihr W-LAN-Netz mit WPA schützen. Die Wi-Fi-Alliance **www.wi-fi.org** – die Zertifizierungsstelle für neue Funknetz-Standards – empfiehlt den Verschlüsselungsstandard für alle Funknetze. Viele Hersteller liefern ihre Geräte mit dem neuen Protokoll aus; ältere Geräte können WPA per Update erlernen. Einrichten muss man die Sicherung aber per Hand. Im privaten Bereich kommt die Variante WPA-PSK (Pre Shared Key) zum Einsatz. Dabei legen Sie ein Master-Kennwort fest, mit dem der PC die Daten verschlüsselt. Der Unterschied zur alten Technik liegt im Detail: Bei WPA wechselt der Rechner die Schlüssel mit jedem Datenpaket. Diese Funktion namens TKIP (Temporal Key Integrity Protocol) macht es Angreifern fast unmöglich sich einzuhacken.

So geht's: Als Beispiel verwenden wir einen Access Point von DrayTek (**www.draytek.de**) und einen USB-W-LAN-Adapter von Netgear (**www.netgear.de**). Getestet haben wir das Vorgehen bei mehreren APs; die Vorgehensweise ist bei anderen Herstellern im Prinzip gleich. Verbinden Sie einen PC per Netzwerkkabel mit dem AP und öffnen Sie den Internet Explorer. Rufen Sie dann die IP des Access Points auf, die Sie auf der Unterseite des Gerätes finden, meist „192.168.0.1“ und gehen Sie in die Rubrik „Funknetz“. Klicken Sie dort auf „Grundeinstellungen“; tragen



4 | SICHER IST SICHER: Für alle Funknetze ist Sicherheit das A und O. Verwenden Sie deshalb für Ihr W-LAN immer den sicheren Verschlüsselungsstandard WPA.



4 | SICHERHEITSLÜCKE WEP: Der veraltete Standard WEP lässt sich mit Hilfe kleiner Programme schnell knacken. Verwenden Sie diese Codierung deshalb nicht mehr für Ihr W-LAN.

Wirklich ruhig schlafen kann aber nur, wer statt WEP das weitaus stärkere WPA verwendet, am besten auch in Kombination mit den anderen Sicherungen. Die Arbeit für das Upgrade von Windows und der Treiber lohnen in jedem Fall.

6 So richten Sie die Clients ein

Wenn Sie einen Rechner ohne SP2 besitzen, benötigen Sie noch ein XP-Update, bevor Sie sich in das Netz einloggen. Gehen Sie auf die Seite **http://windowsupdate.microsoft.com** in die Rubrik „Windows“ und installieren Sie das Update „KB826942-Windows XP-Supportpatch für Wireless Protected Access“. Weitere Informationen zu dem Patch gibt Microsoft unter der URL **http://support.microsoft.com/?kbid=826942**. Klicken Sie dann in der Taskleiste mit der rechten Maustaste auf das Netzwerksymbol und wählen Sie „Verfügbare drahtlose Netze anzeigen | Erweitert“. Aktivieren Sie „Windows zum Konfigurieren der Einstellungen verwenden“. Suchen Sie Ihren W-LAN-Namen aus und klicken Sie auf „Konfigurieren“. Unter „Netzwerkauthentifizierung“ wählen Sie „WPAPSK“ als „Datenverschlüsselung“ und aktivieren „TKIP“. Geben Sie Ihr Kennwort ein und bestätigen Sie mit „OK“. User, die einen Rechner mit SP2 besitzen, klicken mit der rechten Maustaste auf das Netzwerksymbol in der Systray und wählen „Verfügbare drahtlose Netze anzeigen“. Im neuen Fenster markieren Sie das gewünschte Netzwerk und klicken auf „Verbinden“. Nach der Eingabe des WPA-Kennworts sind Sie mit dem W-LAN verbunden.

7 Nicht W-LAN-fähige Geräte ans Netz bringen

Viele Geräte, wie beispielsweise Spielekonsolen besitzen einen Ethernet-Anschluss, aber keinen W-LAN-Adapter, aber da können wir nachhelfen. Alles, was Sie brauchen, ist eine Bridge, etwa die Netgear WGE101. Sie bringt kabelgebundene Netzwerk-Komponenten an das WLAN. Für die Playstation 2 brauchen Sie zudem noch einen Ethernet-Adapter (bei Quelle für 40 Euro).

So geht's: Einstellungen am PC: Stellen Sie eine direkte, drahtlose Verbindung zwischen Bridge und PC her, also ohne den Umweg über einen Router. Installieren Sie den „Smart Navigator“ von der Installations-CD der Bridge. Öffnen Sie den Navigator, klicken Sie auf „Scan“ und wählen Sie die Bridge aus. Wenn die IP-Adresse der Bridge im Netzwerk bereits verwendet wird, ändern Sie sie: Drücken Sie auf „Advanced Settings“ und übernehmen Sie die vom Assistenten vorgeschlagenen Werte. Bei der Anmeldung geben Sie „admin“ als Name an, als Kennwort tippen Sie „password“ ein. Klicken Sie auf „Wireless Network Available“ und aktivieren Sie das gewünschte Netzwerk in der Liste. Wählen Sie „Select“. Nun müssen Sie noch Angaben zum W-LAN machen: Wählen Sie unter „Regulatory Domain“ den Punkt „Europe“ aus; unter „Security Settings “ nehmen Sie „WEP Data Encryption “ und geben das Netzkennwort des AP ein. Bestätigen Sie mit „Apply“. Im Menüpunkt „IP Settings“ markieren Sie „Obtain an IP address automatically “ und klicken wieder auf „Apply“. Unter „Change Password“ können Sie nun ein eigenes Kennwort eingeben, das den Zugriff auf die Konfiguration sperrt. Einstellungen an der Konsole: Bei der Xbox setzen Sie im Menü „Einstellungen | Netzwerkeinstellungen | IP-Adressen“ unter „Konfiguration“ den Schalter auf „Automatisch“. Bei der Playstation belassen Sie die Standard-Einstellungen – dem Spielspaß steht nichts mehr im Weg. Fabian von Keudell

6 | W-LAN GANZ EINFACH: Um sich in ein vorhandenes W-LAN einzuwählen, markieren Sie unter Windows XP einfach das gewünschte Netz und klicken auf „Verbinden“.

PROFI-TIPP

Notebook-W-LAN reparieren

Wenn der Computer mal nicht so will wie sein Benutzer, ist die Fehlersuche oft schwierig. Die kryptischen Fehlermeldungen helfen meist auch nicht weiter.

So ist es auch bei einem W-LAN-Problem, das bei den aktuellen Centrino-Modellen auftritt: Der eingebaute W-LAN Adapter verbindet sich anstandslos mit dem Access Point, doch bei dem Versuch, eine Webseite aufzubauen, erscheint die Meldung „Eingeschränkte Konnektivität“. CHIP zeigt, was dahinter steckt und wie Sie das Problem beheben können.

Energieversorgung zickt In diesem Fall ist die Energieversorgung des Notebook schuld. Die Centrino-Architektur schickt im Akkubetrieb die W-LAN-Karte nach kurzer Zeit in den Schlafmodus, was zu den beschriebenen Schwierigkeiten führt. Einen Patch gibt es leider noch nicht, eine Lösung allerdings schon.

So geht's: Klicken Sie im Menü „Start“ auf „Systemsteuerung“ und dort auf „System“. Im Reiter „Hardware“ drücken Sie auf „Geräte-Manager“ und öffnen den Unterpunkt „Netzwerkadapter“ in der untenstehenden Auswahlliste. Klicken Sie dann mit der rechten Maustaste auf Ihre Wireless-Netzwerkkarte und wählen Sie aus dem Kontextmenü „Eigenschaften“ aus. Unter „Energieverwaltung“ entfernen Sie jetzt den Haken vor „Computer kann Gerät ausschalten, um Energie zu sparen“. Bestätigen Sie die Einstellungen mit „OK“ und starten Sie den PC neu.

Eventuell müssen Sie sich nun erneut mit dem Funknetzwerk verbinden. Klicken Sie dazu in der Systray des Rechners auf das kleine W-LAN-Symbol und wählen im nun erscheinenden Fenster das gewünschte Netzwerk aus.

Wenn's immer noch hakt Sollten sich Ihre Rechner nicht mit dem Netz verbinden, klicken Sie im linken Teil des Fensters auf „Erweiterte Einstellungen ändern“ und gehen in den Reiter „Drahtlosnetzwerke“. Entfernen Sie alle Einträge unter „Bevorzugte Netzwerke“, indem Sie die einzelnen Punkte markieren und auf „Entfernen“ klicken. Bestätigen Sie die Einstellungen mit „OK“. Jetzt sollten Sie sich wieder ganz normal zu Ihrem Funknetz verbinden können.

W-LAN perfekt konfigurieren

Netz-Ressourcen freigeben

Nicht nur der Internet-Zugang lässt sich in einem Netzwerk gemeinsam nutzen, auch das Datei- und Drucker-Sharing ist sinnvoll. Allerdings müssen Sie diese Ressourcen vorher erst freigeben. In diesem Beitrag erfahren Sie, wie Sie die verschiedenen Freigaben einrichten, ohne dass dabei die Sicherheit zu kurz kommt.

In einem Netzwerk teilen sich die Benutzer die Ressourcen und profitieren davon erheblich. Einer der großen Vorteile eines lokalen Netzwerks ist die gemeinsame Nutzung von Dateien, Hardware und Software. Nachdem Sie Ihr drahtloses Netzwerk eingerichtet haben, sollten Sie gleich darangehen, die gemeinsame Nutzung von Dateien und Ordnern zu konfigurieren. Danach können Sie auf einem Rechner im Netz Dateien speichern oder von dort auf Ihren Computer kopieren. Mehr noch: Verfügen Sie über einen Rechner mit einer großen Festplatte, können Sie ihn als zentralen Datei-Server verwenden und dort etwa alle Dokumente, Fotos, Musik- und Video-Dateien speichern, die auch andere verwenden dürfen.

Datei- und Druckerfreigabe aktivieren

Zum Aufbau von Peer-to-Peer-Netzen wird die Datei- und Druckerfreigabe unter Windows XP standardmäßig installiert und aktiviert. Dazu ist die Freigabe des lokalen Ordners „Gemeinsame Dokumente“ erforderlich. Falls Sie aus Sicherheitsgründen die Freigabe von Ressourcen verhindern wollen, können Sie entweder diesen Dienst deaktivieren oder bei der Windows XP Professional Edition mit Hilfe der Gruppenrichtlinien die Nutzung einschränken.

1. Öffnen Sie das Fenster „Netzwerkumgebung“.
2. Ein Klick auf „Netzwerkverbindungen anzeigen“ bringt Sie zum Fenster mit den Netzwerkverbindungen.
3. Klicken Sie mit der rechten Maustaste auf das Symbol für das lokale Netzwerk. Wählen Sie die Option „Eigenschaften“.
4. Aktivieren Sie die Option „Datei- und Druckerfreigabe für Microsoft-Netzwerke“. Klicken Sie dann, je nach Ihrer Absicht, auf „Installieren“ oder „Deinstallieren“.

Einzelne Dateien und Ordner freigeben

Nachdem Ihr Computer Teil des lokalen Netzwerks geworden ist, hat er Zugang zu den freigegebenen Hardware-, Software- und Informationsressourcen, die sich auf den anderen Rechnern im Netzwerk befinden oder daran angeschlossen sind.

CHIP → DVD-CODE Administration

- **Freigaben verwalten** Die Software-Sammlung AdmWin enthält unter anderem den Setup Batcher, der es ermöglicht, Batch-Freigaben zu erstellen und zu verwalten.
- **Unsichere Freigaben finden** Auf der Heft-DVD finden Sie das Tool Winfingerprint mit dem Sie in NT-Domänen oder Active-Directory-Umgebungen unsichere Freigaben suchen.

Auch auf Ihrem Rechner können Sie festlegen, welche Hardware, Dateien und Ordner Sie freigeben wollen, damit sie von anderen genutzt werden können. Windows XP bietet Ihnen ein paar Hilfen für die Freigabe von Dateien, einschließlich des Ordners „Gemeinsame Dokumente“, durch den es sehr einfach ist, Dateien mit anderen zu nutzen.

Das Betriebssystem hat für jeden Benutzer einen Ordner namens „Eigene Dateien“ angelegt. Darin befinden sich Unterordner für „Eigene Bilder“, „Eigene Musik“, „Eigene Videos“, „Eigene eBooks“ und „Eigene Web-Seiten“.

Zum Freigeben einer Datei oder eines Ordners haben Sie mehrere Möglichkeiten. Zunächst einmal können Sie auf Ihrem Rechner jeden beliebigen Ordner freigeben. Um Ihnen die Arbeit zu erleichtern, hat Windows bereits den Ordner „Gemeinsame Dokumente“ eingerichtet und für das Netzwerk freigegeben. Befindet sich der freizugebende Ordner in einem anderen Ordner, der nicht freigegeben ist, können Sie diesen in den Ordner „Gemeinsame Dokumente“ verschieben oder eine Kopie von ihm einfügen.

Zur Ordner-Freigabe unternehmen Sie diese Schritte:

1. Starten Sie den Windows Explorer und öffnen Sie den Ordner „Gemeinsame Dokumente“.
2. Legen Sie einen neuen Ordner mit dem Befehl „Neu“ im Menü „Datei“ an und wählen Sie anschließend die Option „Ordner“ aus
3. Vergeben Sie einen Ordnernamen.
4. Klicken Sie mit der rechten Maustaste auf den neuen Ordner und wählen Sie die Option „Freigabe und Sicherheit“ aus dem aufklappenden Kontextmenü.
5. Aktivieren Sie auf der Registerkarte „Freigabe“ im Bereich „Netzwerkfreigabe und -sicherheit“ das Kontrollkästchen vor „Diesen Ordner im Netzwerk freigeben“.
6. Zur besseren Orientierung der anderen Benutzer können Sie, abweichend vom Ordnernamen, dem Verzeichnis noch einen Freigabenamen zuweisen.
7. In vielen Fällen ist es nützlich, den anderen Benutzern Änderungen an den Dateien zu untersagen. Deaktivieren Sie dann die Option „Netzwerkbenutzer dürfen Dateien verändern“. Bedenken Sie aber, dass in diesem Ordner dann keine Änderungen wie beispielsweise Spielstände oder Ergebnislisten gespeichert werden können.
8. Klicken Sie anschließend auf den Button „OK“. Unter dem Symbol des Ordners wird Ihnen nun eine ausgestreckte Hand angezeigt, ein Zeichen dafür, dass dieser Ordner im Netzwerk freigegeben ist. Falls Sie die Hand nicht sehen, drücken Sie die Taste [F5].

Die besten Netzwerk-Tipps im Web

Support von Microsoft → support.microsoft.com
Technische Ressourcen zur Selbsthilfe
IT-Forum → www.administrator.de
Knowledge-Base für Netzwerk-Administratoren
Windows-FAQ → www.winfaq.de
Professionelle Fragen und Antworten zum Betriebssystem
Windows-Know-how → www.windows.de
Breitgefächertes Wissensportal für Windows-Anwender

9. Überprüfen Sie von einem anderen Computer im Netzwerk, ob der Ordner auch wirklich sichtbar und zugänglich ist.

Einen Drucker im Netz freigeben

Unter Windows 2000 oder XP kümmert sich ein Print-Server um das Drucken der Dokumente. Damit besteht die Möglichkeit, die Druck-Jobs zu verwalten und etwa Benutzer in der Warteschlange zu verschieben oder die Zeiten zu bestimmen, wann ein Drucker online ist. In der Standardeinstellung sind unter Windows XP Home Edition installierte Drucker nicht freigegeben. Sie können jedoch jeden auf dem Computer installierten Drucker freigeben. Dazu gehen Sie folgendermaßen vor (je nach Konfiguration des Startmenüs können geringfügige Abweichungen bestehen):

1. Öffnen Sie die Systemsteuerung und aktivieren Sie das Applet „Drucker und andere Hardware".
2. Klicken Sie anschließend auf „Installierte Drucker und Faxdrucker anzeigen".
3. Klicken mit der rechten Maustaste auf den Drucker, den Sie freigeben wollen, und wählen Sie die Option „Freigabe"

Die auf der Registerkarte „Freigabe" angezeigten Optionen sind unterschiedlich, je nachdem, ob die Freigabe auf Ihrem PC aktiviert ist. Für weitere Anweisungen klicken Sie auf die Option, die Sie auf der Registerkarte „Freigabe" lesen können. **Wenn Sie die** Druckerfreigabe aktivieren müssen, klicken Sie auf den entsprechenden Link, starten den Assistenten und folgen den Anweisungen.

Wird Ihnen eine Option für die Freigabe des Druckers angezeigt, klicken Sie auf „Drucker freigeben" und geben einen Namen für den Drucker ein.

Falls Sie einen Drucker für unterschiedliche Hardware oder Betriebssysteme freigeben wollen, klicken Sie auf „Zusätzliche Treiber" und installieren Sie die erforderliche Software. Klicken Sie anschließend auf „OK".

Wenn Sie die Schritte ausgeführt haben und den Drucker immer noch nicht freigeben können, sollten Sie die Windows-Firewall öffnen. Klicken Sie in der Systemsteuerung auf das Applet „Netzwerk- und Internetverbindungen" und anschließend auf „Windows-Firewall". Aktivieren Sie danach auf der Registerkarte „Ausnahmen" das Kontrollkästchen „Datei- und Druckerfreigabe".

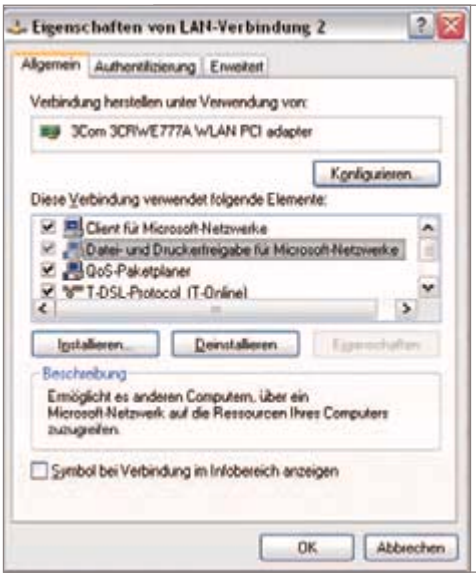
Gemeinsame Dateien im Netzwerk nutzen

Um unter Windows XP auf den Inhalt der gemeinsamen Netzwerkordner zuzugreifen, nehmen Sie die folgenden Arbeitsschritte vor.

1. Öffnen Sie das Fenster „Netzwerkumgebung".
2. Klicken Sie unter „Netzwerkaufgaben" auf die Option „Arbeitsgruppencomputer anzeigen". Das Betriebssystem zeigt Ihnen nun die Computer der eigenen Arbeitsgruppe. Um zu den Computern anderer Arbeitsgruppen zu gelangen, benutzen Sie die Adresszeile unterhalb der Menüleiste.
3. Klicken Sie zweimal auf den Computer, mit dem Sie eine Verbindung herstellen wollen.
4. In den meisten Fällen werden Sie an dieser Stelle nach einem Benutzernamen und einem Passwort gefragt. Nach der Eingabe steht der Nutzung der im Netzwerk freigegebenen Ordner oder Laufwerke nichts mehr im Weg.

Individuelle Zugriffsrechte mit XP Pro

Anders sieht es aus, wenn Sie unter XP Professional für jeden Ordner individuelle Zugriffsrechte festlegen wollen. Um das zu bewerkstelligen, muss man über etwas Spürsinn verfügen, denn diese Funktion ist gut versteckt. Falls noch nicht geschehen, deaktivieren Sie zunächst die allgemeine Dateifreigabe. →



OBLIGATORISCH: Damit die Freigaben im Netzwerk funktionieren, müssen Sie grundsätzlich die „Datei- und Druckerfreigabe für Microsoft-Netzwerke" aktivieren.

Eigenschaften von Spiele
Allgemein
Freigabe
Anpassen
Lokale Freigabe und Sicherheit
Klicken Sie auf diesen Ordner, und ziehen Sie ihn in den Ordner Gemeinsame Dokumente, um den Ordner nur für Benutzer dieses Computers freizugeben.
Aktivieren Sie folgendes Kontrollkästchen, um den Ordner und dessen untergeordnete Ordner nicht freizugeben.
Diesen Ordner nicht freigeben
Netzwerkfreigabe und -sicherheit
Aktivieren Sie das erste Kontrollkästchen, und geben Sie einen Freigabenamen ein, um diesen Ordner für andere Benutzer dieses Computers und im Netzwerk freizugeben.
Diesen Ordner im Netzwerk freigeben
Freigabename: Spiele
Netzwerkbenutzer dürfen Dateien verändern
Weitere Informationen über Freigabe und Sicherheit
OK
Abbrechen
Übernehmen

FREIER ORDNER: Im Kontextmenü des freizugebenden Ordners wählen Sie „Freigabe und Sicherheit" und aktivieren auf der Registerkarte „Freigabe" die Option „Diesen Ordner im Netzwerk freigeben".

1. Starten Sie den Windows-Explorer und markieren Sie den Ordner, dessen Zugriffsrechte Sie definieren wollen.
2. Klicken Sie auf das Menü „Extras“ und wählen Sie die Option „Ordneroptionen“ aus.
3. Aktivieren Sie die Registerkarte „Ansicht“ und deaktivieren Sie unter „Erweiterte Einstellungen“ das Häkchen vor „Einfache Dateifreigabe verwenden (empfohlen)“.
4. Klicken Sie auf „OK“, um das Fenster zu schließen.
5. Klicken Sie mit der rechten Maustaste auf den Ordner, der für einen bestimmten Benutzer freigegeben werden soll, und wählen Sie die Option „Freigabe und Sicherheit“.
6. Aktivieren Sie die Registerkarte „Sicherheit“ und legen Sie für einen Benutzer oder eine Gruppe die Berechtigungen fest.
7. Klicken Sie auf „OK“ und schließen Sie alle Dialogfenster.

Verknüpfungen zu anderen Ressourcen herstellen

Im Fenster „Netzwerkumgebung“ zeigt Ihnen XP die auf den anderen Rechnern im Netz freigegebenen Drucker, Laufwerke, Ordner und Dateien an. Diese Stelle ist außerdem gut geeignet, Verknüpfungen zu anderen Ordnern im lokalen Netzwerk, aber auch zu Web-Seiten oder beispielsweise FTP-Servern im Internet zu speichern.

Um eine Verknüpfung zu einer anderen Netzwerk-Ressource herzustellen, folgen Sie diesen Schritten:
1. Öffnen Sie das Fenster „Netzwerkumgebung“.
2. Klicken Sie unter „Netzwerkaufgaben“ auf die Option „Netzwerkressource hinzufügen“. Der Dialog mit dem „Assistenten für Netzwerkressourcen“ startet. Klicken Sie auf „Weiter“.
3. Wenn Sie gefragt werden „Wo soll diese Netzwerkressource erstellt werden?“, klicken Sie auf „Eine andere Netzwerkressource auswählen“ und anschließend auf „Weiter“.
4. Geben Sie auf der folgenden Seite die Netzwerk- oder Internet-Adresse der Ressource ein oder klicken Sie auf „Durchsuchen“ und danach auf „Weiter“.
5. Soll für die Ressource ein Benutzername und ein Kennwort vergeben werden, haben Sie anschließend Gelegenheit, dies vorzunehmen. Verlangt der Server eine anonyme Anmeldung, klicken Sie auf das Kontrollkästchen „Anonym anmelden“.
6. Geben Sie der Netzwerkressource einen Namen und klicken Sie auf „Weiter“.
7. Über den Button „Fertigstellen“ legen Sie die Verknüpfung an. Schließen Sie alle Fenster, um den Vorgang zu beenden.

Im Fenster „Netzwerkumgebung“ erscheint nun das Symbol für die soeben angelegte Verknüpfung.

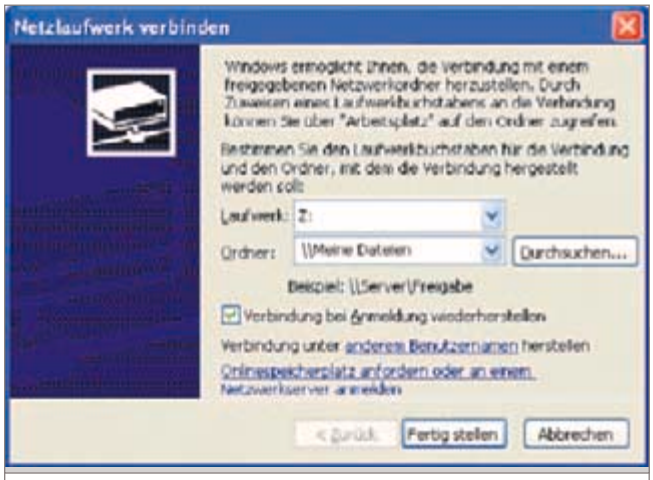
Ordner mit einem Netzlaufwerk verbinden

Als Mitglied einer Arbeitsgruppe können Sie eine Verbindung zu freigegebenen Dateien und Ordnern herstellen. Wenn Sie dieser Verbindung einen Laufwerksbuchstaben zuweisen, können Sie über den Arbeitsplatz auf den Ordner zugreifen. So verbinden Sie unter XP einen Ordner mit einem Netzlaufwerk:
1. Klicken Sie zweimal auf das Symbol „Arbeitsplatz“ auf Ihrem Desktop.
2. Wählen Sie im Menü „Extras“ die Option „Netzlaufwerk verbinden“ aus.
3. Wählen Sie danach einen Buchstaben, der dem Laufwerk zugeordnet werden soll.
4. Geben Sie unter „Ordner“ den Ordner ein, mit dem die Verbindung hergestellt werden soll, oder klicken Sie auf „Durchsuchen“, um den Ordner im Explorer zu finden.
5. Klicken Sie danach auf „Fertigstellen“.
6. Geben Sie noch Ihren Benutzernamen und Ihr Kennwort ein, bevor Sie den Vorgang beenden.

Datei- und Druckerfreigabe beim Service Pack 2

Bestimmte Konfigurationen der Windows-Firewall aus dem XP Service Pack 2 können dazu führen, dass mehr Benutzer auf Ihre freigegebenen Dateien und Drucker zugreifen dürfen, als Sie ursprünglich vorgesehen hatten (siehe auch die Profi-Tipps auf 61). Dennoch ist es möglich, die Datei- und Druckerfreigaben in einem Netzwerk besser zu schützen, wenn Sie die folgenden Empfehlungen berücksichtigen:
Deaktivieren Sie die Datei- und Druckerfreigabe immer dann, wenn Sie eine direkte Verbindung mit dem Internet oder einem nicht sicheren Netzwerk herstellen, zum Beispiel am Flughafen oder in einem Internet-Café.
Installieren Sie einen Router mit Netzwerkadressübersetzung (NAT) zwischen Ihrem PC oder Netzwerk und dem Internet.
Verwenden Sie stets sichere Kennwörter für alle Benutzerkonten und Datei- und Druckerfreigaben. Dies gewährleistet den Lese-, Kopier- und Änderungsschutz der Dateien, die für andere Benutzer verfügbar sind.
Wenn Sie erweiterte Einstellungen der Windows-Firewall vornehmen möchten, finden Sie eine Anleitung auf der TechNet-Website (**www.microsoft.com/technet/default.mspx**).
Installieren Sie in den kommenden Wochen das Update zur Windows-Firewall, sobald es verfügbar ist. Es reduziert das Risiko, dass nicht berechtigte Benutzer auf Ihre freigegebenen Dateien und Drucker zugreifen. Wenn Sie in XP die Funktion für automatische Updates aktiviert haben, bekommen Sie dieses Update ohne weiteres Zutun auf Ihren Rechner.

Halten Sie sich an diese Empfehlungen, um Ihren Computer gegen unbefugte Nutzer abzusichern. Unter Windows XP Service Pack 2 ist die Windows-Firewall standardmäßig aktiviert. Um Ihren Computer vor Viren oder Sicherheitsrisiken zu schützen, sollten Sie diese Einstellung nicht ändern. Durch die Fire-



SCHNELLER ZUGRIFF: Wenn Sie einem freigegebenen Ordner einen Laufwerksbuchstaben zuteilen, können Sie ihn direkt im Arbeitsplatz öffnen.

wall ist die Kommunikation zwischen Ihrem PC und dem Internet eventuell eingeschränkt, in diesem Fall müssen Sie die Einstellungen einiger Programme anpassen. Diese Anpassungen werden als „Ausnahmen“ bezeichnet. Um möglichst hohe Sicherheit für Ihre Daten zu gewährleisten, sollten Sie diese Ausnahmen aber nur mit Vorbehalt einrichten und regelmäßig überprüfen, denn jede Ausnahme in der Windows-Firewall macht Ihren Rechner im Netzwerk anfälliger für Sicherheitsrisiken. Lassen Sie Ausnahmen nur für solche Programme und Dienste zu, die Sie tatsächlich benötigen, und aktivieren Sie diese Ausnahmen auch nur in sicheren Netzwerkumgebungen und nicht in Netzen, die allgemein zugänglich sind.

Vorsicht bei Änderungen an der XP-Firewall!

Beim Aktivieren der Datei- und Druckerfreigabe unter Windows legen Sie eine Ausnahme in der Windows Firewall an. Die ermöglicht anderen Benutzern den Zugang zu den Dateien auf Ihrem PC beziehungsweise zu den daran angeschlossenen Druckern. Wird diese Konfiguration nicht ordnungsgemäß vorgenommen, können auch nicht berechtigte Benutzer Zugriff auf Ihre freigegebenen Dateien und Drucker bekommen. Diese Ausnahme soll jedoch den Zugriff auf die Benutzer beschränken, die an Rechnern in Ihrem Netzwerk arbeiten.

Doch Vorsicht: Die Grenzen Ihres lokalen Netzwerks hängen davon ab, wie Ihr Internet Service Provider (ISP) das Netzwerk konfiguriert hat. So kann etwa ein ganzes Stadtviertel das lokale Netzwerk für einen Breitband-ISP bilden. Je nachdem, wie der ISP die DFÜ-Netzwerkverbindungen konfiguriert, kann sogar das gesamte Internet von der Windows-Firewall als „lokal“ interpretiert werden, sobald Sie die Verbindung über ein Modem herstellen.

Eine Möglichkeit, das lokale Netzwerk auf das gewünschte Ausmaß zu beschränken, besteht darin, die Verbindung zum Internet über einen Router mit Netzwerkadressübersetzung (Network Address Translation, NAT) zu leiten. Am besten ist es, Dateien und Drucker nur dann freizugeben, wenn Sie einen Router mit NAT zwischen Ihren Computer und das Internet geschaltet haben. Ob Ihr Router über NAT verfügt, können Sie seiner Dokumentation entnehmen.

Peter Klau

ABGESTUFT: Unter Windows XP Pro können Sie für jeden Ordner individuelle Zugriffsrechte festlegen – vom Vollzugriff bis zu einfachen Leserechten.

PROFI-TIPPS

Freigaben professionell einrichten

NTFS-Dateisystem nutzen Das NTFS schützt XP-Dateien und -Ordner vor unbefugtem Zugriff. Die Kontorichtlinien regeln, auf welche Funktionen ein Benutzer auf dem PC zugreifen darf. Mit dem Gruppenrichtlinien-Editor existiert ein weiteres mächtiges Werkzeug zum Verwalten von Computer- und Benutzerkonfigurationen, Software- und Windows-Einstellungen sowie administrativen Vorlagen. Mehr Informationen dazu finden Sie über die Windows-Hilfe-Funktion oder auf den Webseiten von Microsoft.

EFS unter XP Pro nutzen Um Ihre Dateien zu schützen, verfügt Windows XP Professional Edition über das Encrypted File System (EFS). Damit können Sie Dateien und Ordner zusätzlich verschlüsseln.

USB-Geräte absichern Zum Sperren des Schreibzugriffs auf USB-Geräte (etwa Memory-Sticks) muss in der Registry der DWORD-Wert für „WriteProtect“ unter „HKEY_ LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies“ von „0“ auf „1“ geändert werden. Sollte der Schlüssel „StorageDevicePolicies“ noch nicht existieren, müssen Sie ihn neu anlegen.

Drucker anders freigeben Sie können einen Drucker auch im Fenster „Drucker und Faxgeräte“ freigeben. Klicken Sie dazu auf den gewünschten Drucker und wählen Sie unter „Aufgaben“ im linken Fensterbereich die Option „Drucker freigeben“. Diese Option ist nur verfügbar, wenn die Ordneransicht so festgelegt ist, dass die Ordner wie eine Webseite aussehen und ein Drucker ausgewählt ist.

XP-Assistent nutzen Der „Assistent zum Hinzufügen von Netzwerkressourcen“ unterstützt Sie beim Anlegen von Verknüpfungen mit anderen Netzwerkressourcen. Klicken Sie zum Starten des Assistenten zunächst im Fenster „Netzwerkumgebung“ auf die Option „Netzwerkressource hinzufügen“.

XP-Firewall ändern Ist die Windows-Firewall aktiviert und sind die Freigaben im Netz nicht zu erreichen, sollten Sie die Datei- und Druckerfreigabe für die Windows-Firewall aktivieren. Klicken Sie im Fenster „Netzwerkumgebung“ rechts auf die Netzwerkverbindung und wählen Sie „Eigenschaften“. Aktivieren Sie die Registerkarte „Erweitert“ und klicken Sie auf „Einstellungen“. Auf der Registerkarte „Ausnahmen“ setzen Sie das Häkchen bei „Datei- und Druckerfreigabe“ und klicken auf „OK“.

Netz-PCs finden Sind bei aktivierter XP-Firewall die Computer einer Arbeitsgruppe nicht auffindbar, aktivieren Sie auf der Registerkarte „Erweitert“ die ICMP-Echoanforderung, und die Computer werden wieder sichtbar.

Leck im SP2 umgehen Trotz aktivierter Firewall lassen sich unter Umständen Dienste sowie Datei- und Druckerfreigaben über das Internet anzeigen und bearbeiten. Selbst wenn die Internet-Freigabe des PCs deaktiviert ist, sind diese Verzeichnisse erreichbar. Die Sicherheit, dass Ihre Daten nur für interne Zwecke freigegeben sind, täuscht. Abhilfe schafft an dieser Stelle das Update für die Windows-Firewall.

Sie können sich aber auch auf diese Weise absichern: Öffnen Sie in der Systemsteuerung das Fenster für die „Windows-Firewall“. Aktivieren Sie auf der Registerkarte „Ausnahmen“ die „Datei- und Druckerfreigabe“. Markieren Sie die gewünschten Ports, klicken Sie auf „Bearbeiten“ und wählen Sie die Option „Bereich ändern“. Die voreingestellte Option „Nur für eigenes Netzwerk (Subnetz)“ funktioniert jedoch nur dann, wenn die Internetverbindungsfreigabe aktiviert ist. Außerdem sollten die Freigaben über den Menüpunkt „Benutzerdefinierte Liste“ nur auf die IP-Adressen des eigenen Netzwerks eingestellt sein.

Wireless Home Office

Kabellos zuhause arbeiten

Surfen und arbeiten in den eigenen vier Wänden, ganz ohne lästige Netzwerkkabel – wenn Sie das schon immer wollten, erfahren Sie in diesem Artikel, wie Sie ein Wireless Home Office einrichten und damit arbeiten. Als Hardware empfehlen sich Notebooks, PDAs und Smartphones.

Ob Sie nun als Telearbeiter oder Freiberufler in den eigenen vier Wänden arbeiten oder sich nur ab und zu Arbeit aus der Firma mit nach Hause nehmen, ein Heim-Netzwerk ermöglicht es Ihnen, sich den für Sie angenehmsten Arbeitsplatz auszuwählen – im Arbeitszimmer, mit einer Tasse Kaffee auf dem Balkon oder sogar im Garten. Die Zeiten, in denen Sie dazu zunächst meterweise Netzwerkkabel durch die Wohnung verlegen mussten, sind vorbei. Denn schon mit wenig Geld können Sie ein drahtloses Netzwerk einrichten, das Ihnen die volle Bewegungsfreiheit in Ihrem privaten Bereich erlaubt.

Mobiles Arbeiten erfordert mobile Geräte

Das erste, was Sie für ein Wireless Home Office benötigen, ist ein mobiler Computer. Doch das muss nicht immer ein Notebook sein; auch andere elektronische Business-Tools können Ihnen helfen, die Verbindung mit dem Rest der Welt aufrechtzuerhalten. Dazu gehören auch Handheld-Computer (PDAs) und Handys (Smartphones).

In vielen Fällen hat nur das Notebook die für die Arbeit nötige Rechen-Power, dafür sind allerdings erhebliche Gewichtsnachteile in Kauf zu nehmen. PDAs und Smartphones verfügen dagegen grundsätzlich über Organizer-Funktionen, etwa Kalender und Adressverwaltung, sowie über eine rudimentäre Textverarbeitung. Die Dateien, die Sie mit den mobilen Geräten bearbeitet haben, können Sie anschließend mit einem Desktop-Computer oder Notebook synchronisieren.

Die Grenzen zwischen den mobilen Geräten sind fließend: Es gibt inzwischen Notebooks, mit denen man telefonieren kann, PDAs, an die Sie eine Tastatur zur Texteingabe anschließen können, und Smartphones zum Surfen im Internet oder zum Versand und Empfang von E-Mails. Obwohl Smartphones und PDAs inzwischen über recht große Displays verfügen, um damit im Web zu surfen, dürfte bei einer komplexen Tabellenkalkulation oder anderen Office-Anwendungen das Notebook das Gerät Ihrer Wahl sein. Die neueste Generation der tragbaren Computer ist leichter, schmaler und leistungsfähiger als ältere Geräte, eine natürliche Grenze bildet an dieser Stelle allerdings die Größe der Tastatur und des Displays.

CHIP → DVD-CODE W-LAN

- **Empfang testen** Mit Hilfe des Network Stumblers testen Sie die Empfangsqualität Ihres drahtlosen Netzes und prüfen ob es Interferenzen durch andere WLANs gibt.
- **PDA-Test** Optimieren Sie Ihren Access Point-Standort besonders flexibel mit dem MiniStumbler für Ihren PocketPC. Er spürt Wireless-Netzwerke auf und testet den Empfang.

Ein drahtloses Heim-Netzwerk einrichten

Es ist grundsätzlich kein Problem, alle im Haushalt vorhandenen Rechner per Funk zu vernetzen. Allerdings ist es für die Administration in vielen Fällen von Vorteil, einen Computer mit einer festen Verbindung zum Access Point (AP) einzusetzen. In der Regel befindet sich der Access Point direkt neben dem PC im Arbeitszimmer. Er fungiert als DSL-Internet-Gateway: Auf der einen Seite ist er mit dem Arbeitsplatzrechner verbunden, ein weiterer Anschluss steht für das DSL-Modem zur Verfügung. Falls noch nicht geschehen, konfigurieren Sie Ihr drahtloses Heim-Netzwerk wie ab 52 beschrieben. Sollte bei der Konfiguration etwas daneben gehen, lassen sich alle Geräte wieder auf die werksseitig verwendeten Werte zurücksetzen.

Für die Verbindung zum Internet müssen Sie die Zugangsdaten Ihres Providers in die entsprechenden Felder eintragen. Verfügen Sie über eine DSL-Flatrate, können Sie die Idle-Time, also die Zeit, nach der eine Verbindung ohne Benutzereingaben unterbrochen wird, nach Ihren Bedürfnissen einstellen.

Bei vielen Access Points lässt sich die Sendeleistung variieren. Möchten Sie etwa nicht, dass das Signal außerhalb Ihres privaten Bereichs empfangen werden kann, können Sie die Sendeleistung verringern. Testen Sie dabei den Empfang mit Network Stumbler (auf DVD). Entscheidungshilfe zur Wahl des Wireless-Standards gibt Ihnen der Kasten auf 63.

Verbindung mit dem Internet aufnehmen

Nachdem Sie herausgefunden haben, welche Geräte Ihren Anforderungen entsprechen, oder diese bereits besitzen, benötigen diese eine drahtlose Verbindung mit dem Rest der Welt. Dazu stehen Ihnen die folgenden vier Technologien zur Verfügung:

WiFi – Standard zur drahtlosen Verbindung von Notebooks und PDAs mit dem Internet.

Wireless WANs – drahtlose Netzwerke, die von mobilen Telefonen benutzt werden, um Sprache und Daten zu übertragen oder im Internet zu surfen.

Infrarot (IR) – drahtlose Verbindung für kurze Entfernungen mit Sichtkontakt. Über Infrarot können Sie Daten, etwa Kontakte und Termine, zwischen zwei Geräten austauschen. Weiterhin können Sie die Infrarot-Schnittstelle dazu nutzen, um Daten mit Ihrem Desktop–PC zu synchronisieren, anstatt das entsprechende Kabel zu verwenden.

Bluetooth – Standard zur Verbindung drahtloser Peripheriegeräte wie beispielsweise Drucker, Digitalkamera, Headset oder

Die besten Home-Office-Tipps im Web

W-LAN und viel mehr → www.tomsnetworking.de
Jede Menge Tests, Workshops, Tipps & Tricks zu allen Themen rund um Netzwerk und W-LAN
Know-how-Fundgrube → www.administrator.de
Zahlreiche Foren zu Netzwerk- und W-LAN-Fragen
LAN, W-LAN & Co. → www.netzwerk-lan.de/de/dept_3.html
Alles, was Sie brauchen, um ein Kabel-Netzwerk um ein W-LAN zu erweitern

Handy mit einem Computer oder zur Vernetzung von Computern über kurze Distanzen (Piconet).

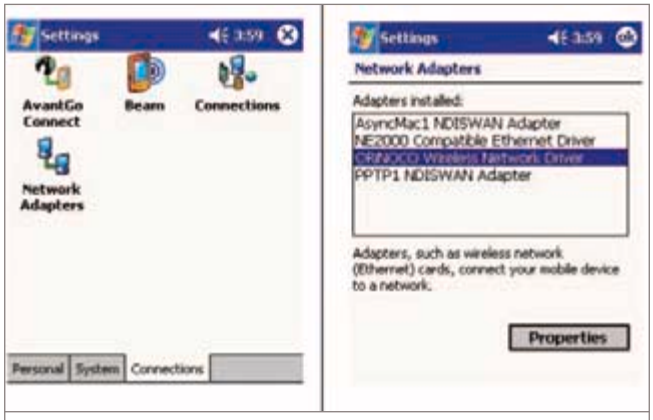
Die drahtlose Netzwerkverbindung einrichten

Um eine WiFi-Verbindung zu einem drahtlosen Netzwerk herzustellen, sollte dieses bereits konfiguriert sein. Die folgende Anleitung gilt für Pocket-PCs und Palm-PDAs.

1. Setzen Sie die W-LAN-Netzwerkkarte in den PDA ein.
2. In der Regel wird ein vorhandenes Netzwerk automatisch erkannt. Ansonsten wählen Sie „Einstellungen | Verbindungen | Netzwerkkarte | Drahtlose | Hinzufügen".
3. Geben Sie auf der Registerkarte „Allgemein" den Netzwerknamen ein.
4. Zum Ändern der Netzwerkeinstellungen markieren Sie das entsprechende Netzwerk in der Liste. Wählen Sie danach aus, ob Sie sich mit einem W-LAN oder dem Internet verbinden wollen, und aktivieren Sie anschließend per Mausklick die Option „Ad-hoc-Verbindung".

Die Authentifizierung konfigurieren

1. Zur manuellen Eingabe der Informationen wählen Sie ein Netzwerk aus und klicken auf das Register „Authentifizierung".
2. Um den Datenverkehr zu verschüsseln, klicken Sie auf „Datenverschlüsselung (WEP-aktiviert)".
3. Für die Shared-Key-Authentifizierung klicken Sie auf „Netzwerkauthentifizierung (Shared mode)".
4. Zum automatischen Einsatz eines Netzwerkschlüssels klicken Sie auf „Schlüssel automatisch bereitgestellt".



RASCH IM NETZ: Unterwegs oder daheim – ein W-LAN-Zugang ist mit dem Pocket-PC schnell eingerichtet. Wählen Sie einfach den passenden Netzwerk-Adapter aus.

5. Eine höhere Sicherheit erreichen Sie durch Aktivieren der Option „Netzwerkzugriff unter Verwendung von IEEE 802.1X". Wählen Sie anschließend den entsprechenden EAP-Typ aus.

Verbindung aufbauen und beenden

Nach der Installation der drahtlosen Netzwerkkarte und dem Einrichten des W-LANs starten Sie das gewünschte Programm, sobald Sie sich im Sende- und Empfangsbereich des drahtlosen Netzes befinden. Um die Verbindung zu beenden, klicken Sie in der Taskleiste auf das Symbol für die Netzwerkverbindung und anschließend auf „Trennen".

Sensible Daten schützen

Mobile Geräte sind sehr attraktiv für Diebe. Häufig sind aber die darauf gespeicherten sensiblen Informationen noch wichtiger als die Hardware. In jedem Fall sollten Sie den Zugang zu den Daten mit einem Passwort schützen. Die Signale in einem W-LAN lassen sich von jedem dazu geeigneten Gerät empfangen, um so wichtiger ist es, alle Schutzmaßnahmen wie Verschlüsselung und VPN zu aktivieren. Mehr zum Thema Sicherheit lesen Sie im Special ab 68. Vorsicht ist auch bei Handys und PDAs mit Bluetooth angebracht. Bei bestimmten Handys ist es möglich, die gespeicherten Daten wie Adressverzeichnisse, Kalender oder Visitenkarte zu manipulieren, ohne dass dies auf dem Handy des Opfers angezeigt wird. Deshalb sollten Sie die Bluetooth-Funktion im Mobiltelefon beziehungsweise PDA grundsätzlich nur in sicheren Umgebungen aktivieren – möglichst nicht an öffentlichen Plätzen wie Bahnhöfen, Flughäfen oder Messen. Aktualisieren Sie die Firmware in regelmäßigen Abständen.

Peter Klau

PROFI-TIPP

Das leisten die verschiedenen W-LAN-Standards

W-LAN nach 802.11b
- Schafft eine Datentransferrate von bis zu 11 MBit/s
- Kann Innenbereiche gut abdecken
- Ist in der Lage, Wände zu durchdringen
- Kann ein bestehendes 802.11b-W-LAN erweitern
- Eignet sich als W-LAN-Zugang für Handheld-Computer
- Reicht aus für eine geringe Anzahl von Benutzern pro Access Point

W-LAN nach 802.11g
- Schafft eine Datentransferrate von bis zu 54 MBit/s
- Kann ein bestehendes 802.11b-Netz erweitern
- Ideal zur Übertragung großer Grafiken oder großer Datenmengen, etwa zur Audio- und Video-Übertragung
- Kann Innenbereiche abdecken
- Kann Wände durchdringen
- Reicht aus für eine geringe Anzahl von Benutzern pro Access Point

W-LAN nach 802.11a
- Schafft eine Datentransferrate von bis zu 54 MBit/s
- Ideal zur Übertragung großer Grafiken oder großer Datenmengen, etwa zur Audio- und Video-Übertragung
- Der richtige W-LAN-Standard, wenn Sie Störungen durch andere drahtlose Geräte vermeiden wollen
- Eignet sich besonders, wenn Sie viele Benutzer pro Access Point haben (Firmen-Lösung)

Funken mit SuSE Linux 9.2

W-LAN mit Linux einrichten

Mit Suse Linux 9.2 kommt endlich mehr Komfort in die W-LAN-Konfiguration. Doch noch ist die Installation eines Funknetzwerks unter Linux nicht ganz ohne Hürden. Dieser Beitrag zeigt Ihnen, wie Sie Ihr W-LAN unter Linux einrichten und häufige Installationsprobleme meistern.

Ein Funknetzwerk unter Linux galt bislang als schwierig zu implementieren. Linux und W-LAN, das war nur etwas für Hartgesottene. Die mussten sich lange durch Konfigurationsdateien und Dokumentation wühlen, bis sie überhaupt an die Einstellungen für das Funknetz kamen. Mit SuSE Linux 9.2 ist das anders. Die vor kurzem erschienene Distribution bietet deutlich verbesserte W-LAN-Funktionen.

SuSE 9.2 unterstützt W-LAN-Karten nach den Standards IEEE 802.11a, 802.11b und 802.11g. Die Standards 802.11b (11 MBit/s) und g (54 MBit/s) sind in Deutschland weit verbreitet.

Ob es für Ihre Karte einen Linux-Treiber gibt, hängt vom verwendeten Chipsatz ab. SuSE 9.2 unterstützt laut Dokumentation folgende Chipsätze in W-LAN-Karten:

Lucent/Agere Hermes
Intel PRO/Wireless 2100
Intersil Prism2/2.5/3
Intersil PrismGT
Atheros 5210, 5211, 5212
Atmel at76c502, at76c503, at76c504, at76c506
Texas Instruments ACX100

Wenn Sie nachsehen wollen, welches Chipset in Ihrer W-LAN-Karte steckt, gehen Sie auf die Webseite **www.linux-wlan.org/docs/wlan_adapters.html.gz** (die Endung .gz funktioniert). Dort finden Sie eine riesige Liste mit so gut wie allen W-LAN-Adaptern und Chipsets.

In einigen Fällen brauchen Sie noch ein Firmware-Update, beispielsweise bei einigen Centrino-Modellen. Das bekommen Sie über das Yast-Online-Update, oder sehen Sie in Yast unter „Software | Software installieren oder löschen“ nach und suchen dort nach „wlan“.

Die W-LAN-Karte installieren

Wenn Sie eine Karte haben, die von SuSE Linux 9.2 unterstützt wird, ist die Installation ziemlich einfach. Stecken Sie die Netzwerkkarte bei laufendem KDE in den PCMCIA-Einschub. Wenige Sekunden später erscheint die automatische Hardware-Erkennung von SuSE. In diesem Beispiel haben wir die Installation mit einer D-Link DWL-G650 PCMCIA-Karte getestet, die auf Anhieb erkannt wurde.

Bestätigen Sie die Meldung mit einem Klick auf „Ja“ und geben Sie im danach erscheinenden Fenster Ihr root-Kennwort ein. Danach startet Yast die Hardware-Erkennung und -Einrichtung. Kurze Zeit später erscheint die neu erkannte Funknetzwerk-Karte markiert in der Liste „Zu konfigurierende Netzwerkkarten“. Klicken Sie anschließend auf „Konfigurieren“.

Grundsätzlich funktioniert die Karte gut mit den Vorgaben im ersten Konfigurationsschritt: DHCP ist voreingestellt, und damit holt sich der Computer seine IP-Adresse und die für eine Verbindung notwendigen Daten vom DHCP-Server.

Im nächsten Fenster des Assistenten müssen Sie schon ein wenig mehr arbeiten. Im allgemeinen gilt als Betriebsmodus „Verwaltet“. Falls Sie jedoch nur zwei Computer direkt per Funknetzwerkkarte verbinden wollen, also ohne Access Point, wählen Sie die Einstellung „Adhoc“.

Geben Sie unter „Netzwerkname (ESSID)“ die Netzwerkkennung Ihres Access Points ein und wählen Sie unter „Authentifikationsmodus“ den Eintrag „Offen“ oder „WPA-PSK“. Die WPA-Verschlüsselung ist sicherer – allerdings kommen noch nicht alle Access Points einwandfrei damit zurecht.

Schließlich geben Sie in der untersten Zeile noch den Schlüssel für den Funknetz-Zugriff ein. Im Normalfall wählen Sie als Eingabeart „Hex“ und tragen genau den Schlüssel ein, den Sie auch in Ihrem Access Point verwendet haben. Falls Ihr Access Point den Schlüssel über eine Passphrase, also ein lesbares Kennwort ermittelt, aktivieren Sie die entsprechende Option und geben Sie dieses Wort ein.

Nach Klicks auf „Weiter“ und „Beenden“ richtet Yast den Funknetz-Zugriff ein. Die Statusleuchten der Funknetzkarte sollten nun blinken und das Funknetzwerk laufen.

Fehler suchen und beseitigen

Hat es nicht auf Anhieb geklappt? Dann gilt es, den Fehler zu finden. Das Mittel der Wahl ist das Programm „iwconfig“, das Sie als Benutzer „root“ aufrufen. „iwconfig“ funktioniert ähnlich wie „ifconfig“, nur eben für Funknetz-Karten. Das Programm liefert nach dem Aufruf ausführliche Informationen über den Verbindungsstatus der Funknetzkarte. Neben der verwendeten Netzwerk-Kennung erhalten Sie auch Aufschluss über die Signalstärke „Link Quality“. Steht dieser Wert auf „0“, haben Sie keine Funkverbindung. Um dieses Problem zu lösen, wechseln Sie Ihren Standort und rufen Sie nach ein paar Sekunden Wartezeit „iwconfig“ noch einmal auf.

CHIP → DVD-CODE W-LAN

- **Top-Wireless-Scanner** Mit dem beliebten Netzwerk-Stumbler Kismet spüren Sie beliebige WLANs in Ihrer Nähe auf, darunter versteckte Netze oder unautorisierte Nutzer.
- **Realistischer Sicherheits-Test** Überprüfen Sie Ihr WLAN auf Sicherheitslücken. AirSnort überwacht den Netzwerkverkehr und kann daraus den WEP-Schlüssel berechnen.

Die besten Linux-W-LAN-Tipps im Web

Übersicht über W-LAN-Chipsätze → http://wiki.uni-konstanz. de/wiki/bin/view/Wireless/ListeChipsatz
Großer Hardware-Katalog und viel W-LAN-Know-how
Basics zum Thema W-LAN unter Linux
→ http://www.holtmann.org/linux/wlan/
Ausführliche Aufbau-Anleitung und viele interessante Links
W-LAN-Extensions → http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.Extensions.html
W-LAN-API mit iwconfig, iwspy und anderen Iw-Tools

Interessant ist auch der Eintrag „Access Point". Falls eine Signalstärke von mehr als „0" angezeigt wird und hinter „Access Point" nur „FF:FF:FF:FF:FF:FF" steht, hat die Karte den Access Point nicht gefunden. Das kann daran liegen, dass der falsche Kanal eingestellt wurde und die Karte den richtigen nicht automatisch gefunden hat. In diesem Fall probieren Sie es von Hand. Starten Sie Yast noch einmal und wählen Sie unter „Netzwerkgeräte | Netzwerkkarte" Ihren Wireless-LAN-Adapter, um dessen Konfiguration zu bearbeiten.

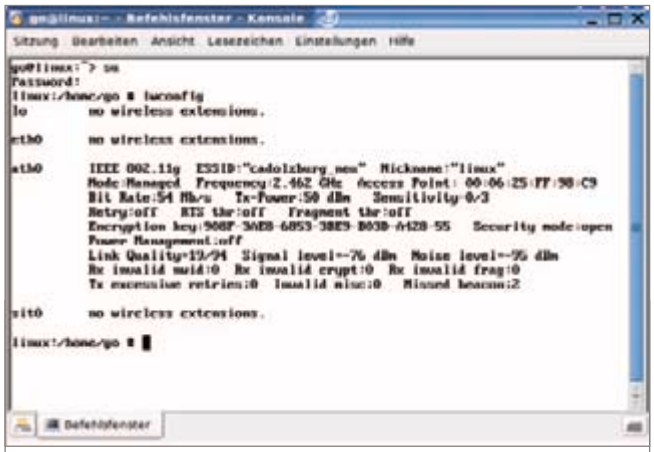
In „Konfiguration der drahtlosen Netzwerkkarte" klicken Sie auf „Einstellungen für Experten". Dort können Sie bei Bedarf einen „Kanal" festlegen. Sehen Sie zuvor in der Konfiguration Ihres Access Points nach, welcher das ist. Im Normalfall ist diese Eingabe aber nicht notwendig, da die Funknetz-Karte im Modus „Verwaltet" automatisch den richtigen Kanal findet.

Nach jeder Änderung rufen Sie „iwconfig" erneut auf und überprüfen die Einstellungen. Scheint alles in Ordnung zu sein, steht also die MAC-Adresse des Access Point in der Liste und ist die Signalstärke ausreichend, sehen Sie nach, ob Ihr Rechner eine vernünftige IP-Adresse bekommen hat. Das geht mit der Eingabe von „ifconfig". Sehen Sie die richtige IP-Adresse? Dann ist alles in Ordnung. Probieren Sie es mit einem „ping" und geben Sie als Zieladresse den Access Point ein, etwa

```
ping 192.168.4.1
```

Der Access Point sollte die Ping-Anfragen beantworten. Passiert das nicht, kann das zwei Ursachen haben:

Sie haben keine IP-Adresse für Ihren Linux-Rechner bekommen – falls dieses Problem auftritt, lesen Sie im nächsten Abschnitt „Das DHCP-Problem" weiter.


Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
Password:
lo no wireless extensions.
eth0 no wireless extensions.
wlan0 IEEE 802.11g ESSID:"cadolzburg neu" Nickname:"linux"
Mode:Managed Frequency:2.462 GHz Access Point: 00:06:25:FF:98:C9
Bit Rate:54 Mb/s Tx-Power:50 dBm Sensitivity=0/3
Retry:off RTS thr:off Fragment thr:off
Encryption key:9087 3AE8 6853 3BE9 D038 A428 55 Security mode:open
Power Management:off
Link Quality=23/94 Signal level=-76 dBm Noise level=-95 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:2
sit0 no wireless extensions.
Befehlsfenster

KONTROLLE: Mit dem Kommandozeilen-Tool iwconfig überprüfen Sie den aktuellen Zustand des Funknetz-Anschlusses.

PROFI-TIPP

Verbindung wiederherstellen

Manchmal kommt es gerade während der Einrichtung eines W-LAN vor, dass eine Verbindung verlorengeht, die zuvor schon funktioniert hatte. Und alles Probieren hilft nichts – das Netz bleibt weg. Da hilft nur der Griff in die Kiste mit den rabiateren Maßnahmen. Probieren Sie es zunächst mit einem so genannten rcnetwork restart.

Damit wird die Netzwerkunterstützung neu initialisiert und der Rechner fordert erneut eine IP beim Access Point an. **Neu konfigurieren** Falls das nicht hilft, spielen Sie in Yast noch einmal die komplette Netzwerkkonfiguration durch. Kontrollieren Sie dabei alle Parameter – vielleicht haben Sie sich beim Schlüssel vertippt. Auch wenn Sie keine Änderungen vornehmen, speichern Sie die Konfiguration nochmals.

System neu starten Die letzte Möglichkeit ist ein kompletter Systemneustart. Das ist vor allem dann sinnvoll, wenn Sie Ihr Funknetz schon eine Weile konfiguriert haben, aber nicht mehr genau wissen, welche Änderung wie gegriffen hat.

Denken Sie auch daran, dass das Problem oft nicht am Linux-Computer liegt. Möglicherweise ist die Funkverbindung unterbrochen oder zu schwach für eine kontinuierliche Übertragung. Dann kommt es oft zu kaum erklärlichen Ausfällen.

Auch der Access Point kann sich einmal verschlucken. Wenn gar nichts mehr geht, schalten Sie den Access Point aus und starten Sie ihn neu.

Sie haben die SuSE-Firewall eingeschaltet. Dann schalten Sie zunächst einmal die Firewall ab; das geht in Yast unter „Sicherheit und Benutzer | Firewall". Natürlich sollten Sie diesen Schutz nicht auf Dauer ausgeschaltet lassen. Nachdem Ihr Netz sauber konfiguriert ist, können Sie die Schutzmauer wieder einschalten. **Tipp:** Achten Sie beim Einrichten der Firewall darauf, dass Sie auch die richtige Schnittstelle schützt, im Falle eines Funknetzwerks also die mit der Bezeichnung „wlan-id-xx:xx:xx:xx;xx;xx".

Das DHCP-Problem lösen

Ist die Funknetzwerkkarte so weit eingerichtet und liefert auch iwconfig gute Werte? Gut. Funktioniert Ping, aber es erscheint keine Website beim Aufruf? Schlecht. Offenbar funktioniert in diesem Fall die Namensauflösung nicht.

Eventuell liegt das Problem in der DHCP-Konfiguration. Das tritt vor allem dann auf, wenn in Ihrem Notebook noch ein Ethernet-Adapter steckt, der auch DHCP-Daten anfordert. Und egal, ob der eine Verbindung hat oder nicht – das stört. Auch das Entfernen des Ethernet-Anschlusses aus der Hardware-Konfiguration von Yast nutzt nichts.

Abhilfe schafft dagegen ein kleiner Eintrag in einer Datei im Verzeichnis „/etc/sysconfig/network/". An dieser Stelle finden Sie eine oder zwei Dateien, die mit „ifcfg" beginnen. Suchen Sie die heraus, die mit „ifcfg-wlan-id" beginnt und die MAC-Adresse der W-LAN-Karte trägt. Öffnen Sie die Datei mit einem Editor und schreiben Sie als letzte Zeile hinein:

```
DHCLIENT_PRIMARY_DEVICE=yes
```

Damit räumen Sie der Karte bei der Vergabe von IP-Adressen eine höhere Priorität ein. Starten Sie mit

```
rcnetwork restart
```

→

das Netzwerk neu. Dabei können Sie beobachten, wie Ihr W-LAN-Client eine DHCP-Adresse bekommt. Und mit dieser Adresse kommen auch die korrekten Daten, die für die Namensauflösung von Internet-Adressen notwendig sind.

Versuchen Sie erneut, von Ihrem W-LAN-Notebook aus ins Internet zu kommen. Jetzt sollte alles funktionieren. Falls nicht, lesen Sie den Kasten „Verbindung wiederherstellen“ auf 65.

Top-Werkzeug: Der KWiFi-Manager

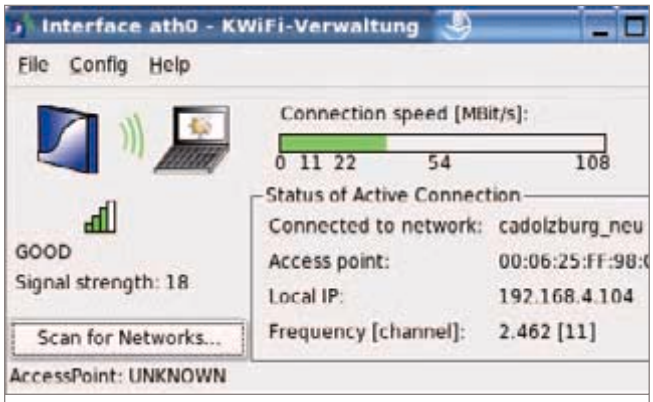
Eine große Hilfe für alle Funknetzwerker ist das Tool KWiFi-Manager. Das finden Sie in Yast unter „Software installieren oder Löschen“. Wählen Sie als „Filter“ die „Suche“ und geben Sie als Suchbegriff „wlan“ ein. Kurze Zeit danach erscheint das Paket „kdenetwork3-wireless“, das Sie anschließend sofort installieren können.

Nach der Installation rufen Sie das Programm über die Tastenkombination [Alt]+[F2] und mit der Eingabe von „kwifimanager“ auf.

Auf dem Bildschirm erscheint ein Kontrollfenster, und rechts unten in der Kontroll-Leiste finden Sie ein kleines Diagramm. Das zeigt die aktuell ermittelte Signalstärke an.

Im Kontrollfenster des Programms sehen Sie neben der Signalstärke auch Informationen über das aktuell gewählte Funknetzwerk, die Verbindungsgeschwindigkeit und die lokale IP-Adresse. Per Knopfdruck auf „Scan for Networks“ lassen Sie Linux nach anderen Funknetzwerken suchen.

Praktisch für die Festlegung des idealen Standorts ist die akustische Suche. Die schalten Sie ein mit „Config | Acoustic Scanning“. Je nach Signalstärke erklingt ein mattes „Plop“ oder – bei besseren Verbindungen – ein begeistertes Piepsen. Das ist



KOMFORT: Mit dem KWiFi-Manager verfügen Sie über ein komfortables Kontroll-Werkzeug für Ihr Funknetz.

nicht nur für Hobby-Wardriver interessant, die auf der Suche nach offenen Funknetzen durch die Stadt fahren. Es ist auch ideal, um die perfekte Position und Antennenausrichtung des Access Point in Erfahrung zu bringen. Sie stellen einfach das Notebook am gewünschten Ort auf, schalten die Akustik ein und drehen es so lange, bis das „Acoustic Scanning“ die vielversprechendsten Geräusche von sich gibt.

Ein weiteres Werkzeug für die Qualitätskontrolle finden Sie unter „File | Connection Statistics“. An dieser Stelle zeigt ein Diagramm den Verlauf der Signalstärke und des Rauschlevels in den letzten vier Minuten an.

Für den Einsatz an unterschiedlichen Orten ist der Manager ebenfalls gerüstet. Bis zu vier Konfigurationen können Sie dem Programm mit auf den Weg geben und bei Bedarf zuschalten –

HARDWARE-TIPPS

W-LAN-Adapter, die sehr gut von Linux unterstützt werden

Abocom 802.11b: CWB 1000, WUB 1500, WMB 2000, WP 2000, WBI 500, WB 1500H, WB 1500S, WB 1500SH, WB 2000, WB 2500, WMB 2500 **802.11g:** WG 2000Ca, WPG 2000, WUG 2200, WG 2400Ca, WMG 2400, WPG 2400
AboveCable 802.11b: ACPC2000
Accton 802.11b: WN 3101J, WN 3101-1, WN 3302A, WN 3304A, WN 3306A, WN 3401B **802.11g:** WN 4201, WN 4301Ca, WN 4401,
Acer 802.11b: 2411, 2413
Acrowave 802.11b: AWL-1100UFD, AWL-1100CF, AWL-1100M, AWL-1100U, AWL-1100P, AWL-1100C
Actiontec 802.11b: 802PI25, 802CI2, 802UI3, HWC01150-01, HWP01170-01, HWU01170-01 **802.11g:** tbd **802.11a:** HWC05490-01
Adaptec 802.11b: AWN 8010, AWN 8020, AWN 8030
Addtron 802.11b: AWP-100, AWA-100, AWP-101, AWU-110, AWU-120
ADMtek 802.11b: ADM8211
Adtec 802.11b: ADLINK 342CF, ADLINK 2422C
AIN Comm 802.11b: AWU 2000b **802.11g:** AWU-2000g
AirLink Tech 802.11b: WLG-1100P, WLG-1100U
Airvast 802.11b: WN-100, WN-100S, WN-110, WN-130, WN-200, WN-210, WN-220, WN-168b, WN-310 **802.11g:** WN-150g, WN-360g **802.11a/g:** XN-100, XN-200
Allnet 802.11b: ALL0181, ALL0182, ALL0183, ALL0183P, ALL0191, ALL0192, ALL0193, ALL0194 **802.11gA:** LL0271, LL0272, LL0273
Aopen 802.11b: 701R, 702R, 701K, 703F,703D
Artem 802.11b: CC-STD-PC-b, CC-EMB-PC-b, CC-PCI, USB-W11 **802.11g:** CC-STD-PC-g
Asus 802.11b: WL-100,WL-103b, WL-110, WL-140 **802.11g:** WL-100G, WL-160G **802.11a/b:** WL-200
Belkin 802.11b: F5D6020, F5D6050, F5D6001, F5D6060 **802.11g:** F5D7000, F5D7010
D-Link 802.11b: DWL-120, DWL-122, DWL-610, DWL-650, DRC-650, DCF-650W, DCF-660W, DWL-660, DWL-500, DWL-510, DWL-520, DWL-650H **802.11g:** DWL-124, DWL-G520, DWL-G650 **802.11a:** DWL-A650, DWL-A520
Dell 802.11b: TrueMobil 1150, TrueMobil 1180
Fujitsu-Siemens 802.11b: E-1100, C-1100, E-5454 **802.11g:** E-5400, E-5454
Gemtek 802.11b: WL-210, WL-211, WL-280, WL-311, WL-613, WL-360, WL-375, WL-379, WL-380/780, WL-388, WL-611, WL-612F, WL-616, WL-672, WL-711, WL-350, WL-352BW **802.11a:** WL-550, WL-511 **802.11g:** WL-360G, WL-780G, WUBI-100GW, WPI-100G, WL-611G, WL-811, WL-818F, WL-850
Hawking Tech. 802.11b: WE110P, WP251, WUI120, WU250, WEI120P, CF100W, WU300, H-WU36D **802.11g:** HWC54G, HWP54G
Hewlett-Packard 802.11b: hn210w, hn220w, WL 210, WL 215, W 200
IBM 802.11b: 09N9904, 22P6901, 22P7701 **802.11a:** 22P7501
Intel 802.11b: AP 311, AP 310, AP 321, WUD 2011B, WPC2011, WPC2011BWW, WPCI2011B, WM3B2100 **802.11g:** WM3B2200BG **802.11a:** WCB5000, WPCI5000PCI

theoretisch. Im Test hat das nicht einwandfrei funktioniert, denn der Manager hat die Konfigurationen wieder verloren.

iw-Tools für die Kommandozeile nutzen

Neben dem komfortablen KWiFi-Manager gibt es noch eine Reihe von interessanten Kommandozeilen-Tools. Das Werkzeug „iwconfig“ haben Sie bereits kennengelernt. Es hilft, die Netzwerkverbindung zu kontrollieren und einzurichten. Das Programm stammt aus einem Paket, das noch weitere Utilities für Linux-Funknetzwerker enthält:

„iwspy“ liefert Verbindungsstatistiken. Dazu geben Sie die verwendete Netzwerkschnittstelle und eine Zieladresse an, beispielsweise die eines anderen Rechners. Danach ermittelt der SuSE-Spion alle möglichen Daten über die Verbindungsgeschwindigkeit und -qualität. Das funktioniert allerdings nicht mit allen W-LAN-Karten.

„iwlist“ holt detaillierte Informationen über verfügbare Funknetzwerke ein. Dazu geben Sie zum Beispiel ein

```
iwlist ath0 scan
```

Zurück bekommen Sie eine Liste aller in Funkreichweite verfügbaren Access Points. Zusätzlich erscheinen Informationen darüber, ob die Übertragung verschlüsselt ist und wie stark die Verbindung ist.

Oder möchten Sie vielleicht wissen, welche Schlüssellängen Ihre W-LAN-Karte unterstützt? Dann geben Sie ein

```
iwlist ath0 key
```

und Sie erhalten die verfügbaren Schlüssellängen sowie die von Ihrer W-LAN-Karte verwendeten Schlüssel.

„iwevent“ schreibt alle auftretenden Events mit, die mit Wireless LAN zu tun haben. Dazu zählen zum Beispiel verlorene und wiederaufgenommene Verbindungen.

„iwpriv“ zeigt, welche speziellen Kommandos ein W-LAN-Adapter versteht und erlaubt, diese zu manipulieren.

Mehr über diese Funktionen erfahren Sie, indem Sie die jeweiligen Manual-Seiten öffnen.

Eine weitere Informationsquelle für die aktuelle Verbindung ist /proc/net/wireless. Mit

```
cat /proc/net/wireless
```

rufen Sie die aktuellen Informationen über Ihre W-LAN-Schnittstelle ab.

Fazit: In Sachen W-LAN ist SuSE mit der Version 9.2 ein großer Schritt nach vorne gelungen. So komfortabel wie mit Windows funktioniert W-LAN zwar noch nicht – aber endlich kann man auch Linux mit wenig Aufwand kabellos vernetzen.

Martin Goldmann

KNOW-HOW

Infos zu Linux-Funknetzen

Mehr Informationen zum Thema W-LAN und Linux gibt es in Linux selbst und vor allem im Internet. Das sind die wichtigsten Quellen:
Mit der Eingabe von

```
man wireless
```

erhalten Sie einen guten Überblick über die Tools zur Netzwerk-Überwachung und zur Konfiguration. Wichtige Fakten zur Einrichtung Ihres W-LAN in SuSE Linux verrät die Online-Hilfe von SuSE 9.2. Klicken Sie einfach auf den Rettungsring in der Taskbar von KDE und geben Sie als Suchbegriff „WLAN“ ein. In Kapitel 17 des Administrationshandbuchs werden Sie ebenfalls fündig.

Lancom 802.11b: MC-11, PCI-11, USB-11 **802.11g:** MC-54g **802.11a:** PCI-54a
LanReady 802.11b: CEW-7106PC, WB 2000, WUB 1500, WP 2000, NL-2511CD Plus, EW-7117U **802.11g:** CNL-3054CB, WE-601-I, WPG 2000
Linksys 802.11b: WPC11, WMP11, WUSB11, WET11, WCF11, WCF12, WUSB12 **802.11a:** WPC54A **802.11g:** WUSB54G, WMP54G, WPC54G
Microsoft 802.11b: MN-510, MN-520 **802.11g:** MN-720, MN-730
MSI 802.11b: UB11B, PC11B, CB11B **802.11g:** PC54G, MP54G
NDC 802.11b: NWH1012, NWH3012, NWH4011, NWH4020, NWH4010, NWH1010 **802.11g:** NWH3050, NWH1050, NWH3051
Netgear 802.11b: NWH4011, MA 111, MA 311, Ma 401, MA 401RA, MA 521, MA 701 **802.11a:** HA 501, HA 311 **802.11g:** WG 121, WG 311, WG 511, WG 511T
Planex 802.11b: GW-NS110, GW-NS110PX, GW-NS11R, GW-NS11H, GW-NS11S, GW-NS11C, GW-NS11X, GW-US11H, GW-US11S, GW-US110, GW-CF11H, GW-CF110, GW-DS11C **802.11a:** GW-NS540a **802.11g:** GW-NS54G, GW-DS54G
Proxim 802.11b: 7230, 7431, 7432, 7630, PC24E-00-ET, PC24E-H-ET, 8110, 8410, 8420-WD, 8421, 8424-WD, 8430, 8432, 8433-05, 8434-05, 8630 **802.11a:** PN 4030, 8450, 8451 **802.11g:** 8470, 8471
Samsung 802.11b: SWL-2000N, SWL-2000P, SWL-2100E, SWL-2100N, SWL-2100P, SWL-2100U, SWL-2200C, SWL-2200U, SWL-2200P, SWL-2210P, SWL-2210M, SWL-2300N, SWL-2300P, SWL-2300U, SWL-2300M
Sitecom 802.11b: WL-002, WL-003, WL-010, WL-011, WL-012, WL-015, WL-016 **802.11g:** WL-100b, WL-100i, WL-110b, WL-120, WL-121
SMC 802.11b: 2532W-B, 2632W, 2602W, 2635W, 2642W, 2662W, 2664W **802.11a:** 2735W **802.11g:** 2802W, 2835W
3Com 802.11b: 3CRWE62092A, 3CRWE62092B, 3CRSHPW696, 3CRSHPW196, 3CRDW696, 3CRSHEW696, 3CRWE737A, 3CRWE73796B, 3CRWE777A, 3CRSHPW796 **802.11g:** 3CRWE154G72
Tellus 802.11b: C100, C100A, C120, C125, C126S, F110, F125, TWL-U11, U110, U-111, P120, P125, M120, M125, C130 **802.11g:** C200, C210, M210, C220, M220, P220
TRENDware 802.11b: TEW-221PC, TEW-222CF, TEW-223PI, TEW-224UB, TEW-226PC, TEW-228PCI **802.11g:** TEW-401PC, TEW-403PCI
US Robotics 802.11b: USR2410, USR2415, USR2445, USR1120 **802.11g:** USR5410, USR5416
USI 802.11b: CF-B-AG-01, IXMUSB114401, PC-B-AG-02, PC-B-AG-04 **802.11g:** CB-G-IN-01
Wistron 802.11b: PC-200, PC-250, USB-300, USB-400, CF-100, CB-200B, EM9-NB, EM9-CF, EM-200B **802.11g:** CB-300G, EM-300G
W-Link 802.11b: WEN-2073, WEN-2070, WEN-2050, WEN-2016, WEN-2015, WEN-2013, WEN-2012, WEN-2011, WEN-2010, WEN-2091, WEN-2200 **802.11a:** WEN-2520, WEN-2515, WEN-2510, WEN-2500
Z-Com 802.11b: XI300, XI300B, XI305B, XI325, XI325HP, XI330B, XI360, XI625, XI626, XI725/726, XI735, XI750, XI800, XI815, XI825 **802.11a:** XV5300, XV5325, XV5625 **802.11g:** XG300, XG600, XG900
Zyxel-Zyair 802.11b: B-100, B-120, B-200, B-220, B-300, B-400 **802.11g:** G-100

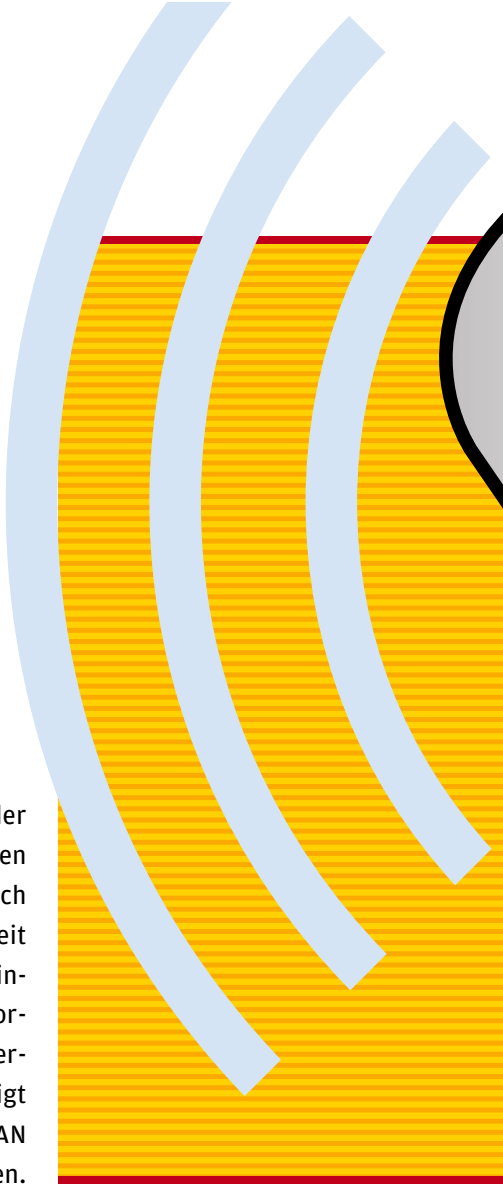
SPECIAL | INHALT

Gefahrensicheres W-LAN 68
Hacker, Sniffer, War-Driver – so schützen Sie Ihr Funk-Netzwerk am besten vor Angriffen.

Hacker aussperren 76
W-LANs ziehen Datenspione magisch an. CHIP verrät die besten Abwehr-Methoden.

10 Tipps fürs sichere Netz 80
WEP oder doch lieber WPA? Wir verraten Ihnen Tipps & Tricks, wie Sie Ihr W-LAN schützen.

Vorsicht, Schwarzsurfer! 83
Wenn ungebetene Gäste in Ihrem Funknetz auf Ihre Kosten surfen, handeln sie oft noch nicht mal strafbar.



So komfortabel der Umgang und das Arbeiten mit drahtlosen Netzen auch ist, beim Thema Sicherheit sollten Sie ganz genau hinsehen. Dieses Special informiert Sie über alle Sicherheitsrisiken und zeigt Ihnen, wie Sie Ihr W-LAN wirkungsvoll schützen.

Gefahren und Risiken für W-LANs

Sicherheit in

Drahtlose Kommunikation erfreut sich aufgrund ihrer Flexibilität und der Verbreitung von mobilen Geräten, die heute in fast jede Tasche passen, sowie der steigenden Datenübertragungsraten immer größerer Beliebtheit. Besonders das Wireless Local Area Network (kurz W-LAN) hat einen wahren Siegeszug in Privat- und Unternehmens-Netzwerken angetreten. Die Vorteile gegenüber einem herkömmlichen, kabelgebundenen Netzwerk sind hinlänglich bekannt: Sie können kabellos im Internet surfen, Dokumente aus dem Netzwerk bearbeiten und den eigenen Arbeitsplatz quasi überall in Reichweite des W-LAN nach Belieben platzieren.

Vor allem Unternehmen bietet das flexible W-LAN eine günstige Alternative zu einer kostspieligen Erweiterung ihrer kabelgebundenen Netzwerkstruktur. Auch waren den Kabelnetzen in der Vergangenheit immer wieder recht enge physikalische Grenzen gesetzt, denn häufig endete der Auf- und Ausbau etlicher Firmen-Netzwerke sprichwörtlich an der Wand.

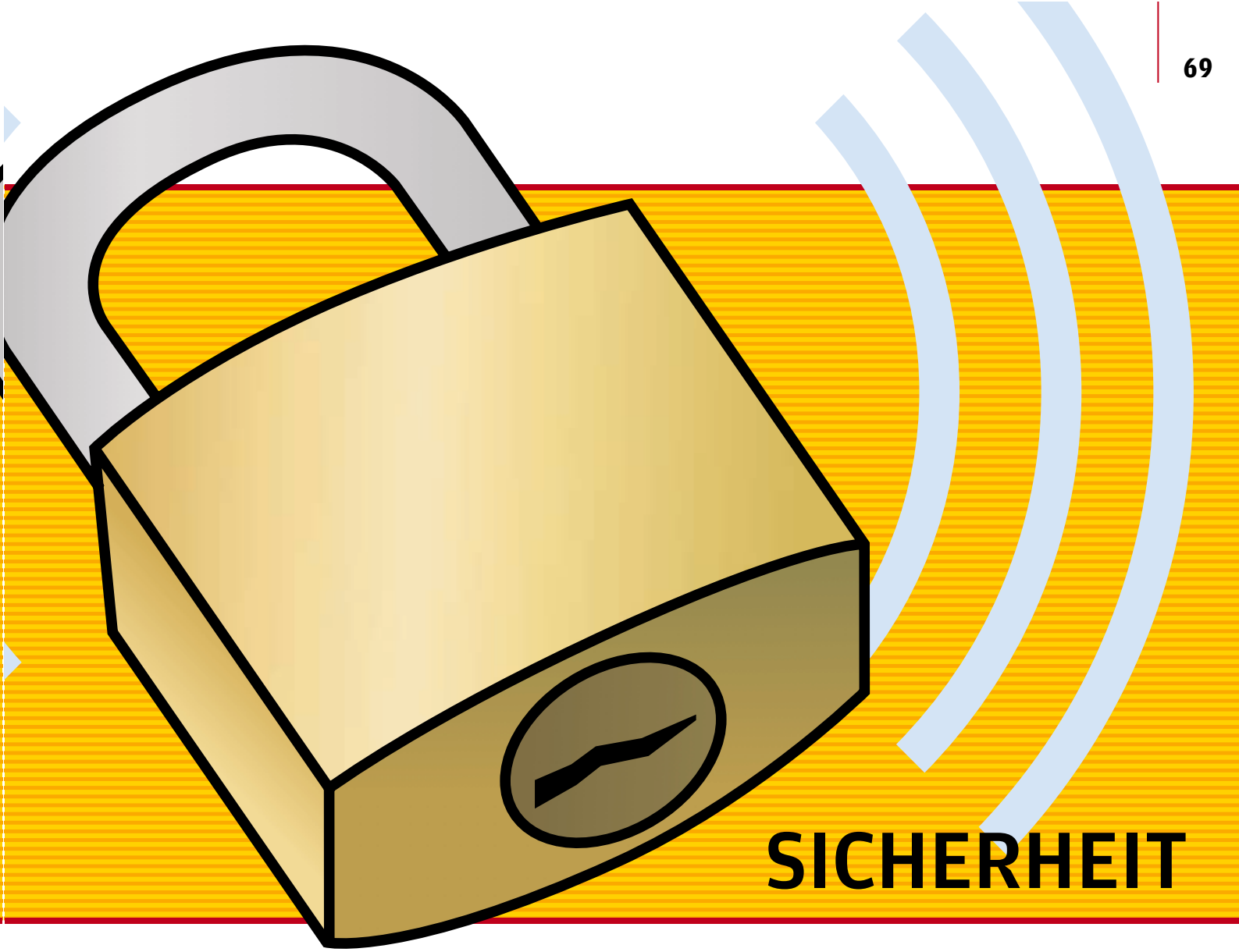
Dank der Wireless-Technologie ist es heute dagegen möglich, Daten auch über größere Entfernungen oder durch Hinder-

CHIP AUTOR → www.mns-security.de

Thomas Vosseberg ist Sicherheitsberater bei der mns-security GmbH. Sein Wissen im Bereich der IT-Sicherheit hat er bereits vielen Administratoren in Security-Trainings vermittelt. Sein Buch „Hackerz Book – neue Techniken, neue Ziele“ (2. Auflage 2003, mit CD, www.hacking-security.de) ist im Franzis Verlag erschienen.

CHIP → DVD-CODE W-LAN

- **Netzwerk-Sniffer** Die Programme Network Stumbler, Aerosol, Ethereal und das Linux-Programm Kismet enttarnen W-LANs und liefern passende Infos.
- **Netze knacken** Die Tools WEPCrack, Airsnort und WPA Cracker decodieren die WEP-Schlüssel, die Sie zur Anmeldung an ein W-LAN benötigen.
- **Pong** Mit dem Tool lassen sich unter anderem von Access Points der Hersteller D-Link und Linksys die WEP-Keys und das Admin-Passwort auslesen.



SICHERHEIT

Wireless Netzwerken

nisse, wie etwa Zimmer- oder Hauswände, hindurch zu übertragen. Hinzu kommt, dass die Mitarbeiter vieler Firmen mit dem Arbeitsmittel PC extrem flexibel sein müssen. So sind sie häufig mit dem Firmen-Notebook unterwegs und benötigen sicheren Zugriff auf ihre Daten oder nutzen beispielsweise eine Bahnfahrt, um Arbeiten mit Hilfe von W-LAN vorzubereiten und zu erledigen. Dafür nutzen sie häufig öffentliche Access Points, die in Hotels, Flughäfen, Bahnhöfen, Restaurants oder auch bei Geschäftspartnern installiert sind. Der Mitarbeiter nutzt dann das W-LAN, um sich beispielweise per Remote Control in das Firmennetzwerk einzuloggen.

Die Schwachstellen der Funknetze

Wie bei fast jeder neuen Technologie wurde zunächst die Funktion entwickelt. Dabei wurde viel Wert darauf gelegt, dass die Einrichtung und Nutzung des W-LAN möglichst einfach und komfortabel vonstatten geht. Nachdem die Begeisterung für die Vorteile der neuen Technologie geweckt war, arbeitete man an der zügigen Beseitigung von Bugs oder Schwachstellen.

Allerdings hatte die schnelle Entwicklung der Funknetze nicht nur positive Folgen: Zahlreiche Bugs und etliche Sicherheitslücken schadeten dem Image von W-LAN, sodass viele Administratoren den Einsatz drahtloser Funk-Netzwerke – trotz ihrer vielen Vorteile – mit dem Verweis auf die mangelnde Sicherheit kategorisch ablehnten.

Bei der Planung, Installation und Administration Ihres Wireless-Netzes sollten Sie sich vor Augen halten, dass W-LAN nicht als Transportmittel für wichtige Daten entwickelt wurde. Daher muss dem Sicherheitsaspekt erhöhte Aufmerksamkeit zuteil werden. Selbst nachträglich in W-LAN integrierte Sicherheitsmaßnahmen wie Wired Equivalent Privacy (WEP) oder die Access-Control-List (ACL) erwiesen sich prinzipiell als unsicher und können mittlerweile mit ausgefeilten Tools von Hackern und War-Drivern ausgehebelt werden.

Insbesondere fehlt beim W-LAN der physikalische Schutz für die zu übertragenden Daten, den im festverbundenen Netzwerk das Kabel bietet. Durch die Funkübertragung werden die Daten-Pakete quasi ungeschützt durch die Luft versendet und breiten →

sich fast unkontrollierbar in der Umgebung aus. Sie können beispielsweise von Dritten empfangen, aufgezeichnet, ausgewertet oder sogar manipuliert werden. Vor allem das Mithören des Netzwerkverkehrs, das so genannte Sniffen, ist eine der größten Gefahren im WLAN.

CHIP zeigt Ihnen, welchen Gefahren und Risiken Ihre Daten mit dem Einsatz eines W-LAN ausgesetzt sind und wie Sie diesem Risiko gezielt entgegenwirken können, sodass War-Driver und Hacker keine Chance haben.

Bequeme Installation auf Kosten der Sicherheit

Die Installation der benötigten Wireless-Endgeräte ist in der Regel recht simpel, sodass auch Anwender ohne spezielle Netzwerkkenntnisse mit ihr zurechtkommen.

Meist reicht es, den Access Point an einer beliebigen Stelle ins lokale Netz einzusetzen oder den W-LAN-Router mit dem Internet zu verbinden. Bei den zugehörigen Wireless-Netzwerkkarten sieht es ähnlich aus, da meistens die Treiber der gängigsten W-LAN-Karten sowie die benötigten Konfigurationstools bereits in Windows XP integriert sind. Daher erkennt das Betriebssystem die W-LAN-Karte in der Regel selbstständig.

Nach der Installation aktiviert das System das Gerät und die Karte beginnt umgehend mit der Suche nach Funknetzwerken in ihrer Reichweite. Da die meisten Access Points werkseitig mit einem aktiven DHCP-Server ausgeliefert werden, der jedem anfragenden Client umgehend eine IP-Adresse im angeschlossenen Netzwerk zuteilt, findet die gerade installierte Netzwerkkarte des Clients selbstverständlich auch sofort den passenden Access Point und kann sich mit ihm verbinden.

Für viele W-LAN-Anwender ist die Konfiguration an dieser Stelle beendet, denn offensichtlich funktioniert ja alles mit den werkseitigen Einstellungen. Doch diese bequeme Installation hat einen gewaltigen Haken: Damit sich die Geräte auf Anhieb verstehen, sind alle relevanten Sicherheitseinstellungen, beispielsweise die WEP-Verschlüsselung oder der MAC-Adressen-Filter, werkseitig deaktiviert.

Andere Anwender sehen sich gegenüber den recht häufig unübersichtlichen Einstellungen, wenig benutzerfreundlichen Treibern, unverständlichen Fachbegriffen, der Vielzahl der Einstellungen und der Inkompatibilität verschiedener Hardware überfordert, sodass sie lieber auf die so wichtigen Sicherheitsmaßnahmen verzichten und das W-LAN lediglich mit den Standardeinstellungen des Herstellers betreiben. So bemerken sie vielleicht nicht einmal, dass sich ihre W-LAN-Karte gerade mit dem Access Point des Nachbarn verbunden hat.

Geschwätzige Access Points

In der Standard-Einstellung des Herstellers sendet ein Access Point ununterbrochen Signale, die so genannten Broadcast-Beacons. Sie werden in regelmäßigen Intervallen ausgesendet, um in der Nähe befindlichen Clients zu signalisieren, dass die aufgebaute Verbindung noch steht beziehungsweise dass es in ihrer Reichweite ein drahtloses Netz gibt. Bei einigen Netzwerken ist dieses Verhalten grundsätzlich erwünscht – denn es erleichtert zum Beispiel den Zugang zum Unternehmens-W-LAN erheblich.

Die im Millisekunden-Takt versendeten Funk-Beacons enthalten alle W-LAN-spezifischen Daten, die ein Client für einen einfachen Verbindungsaufbau benötigt. Der Haken bei der Sache: Nicht nur autorisierte Systeme bekommen diese Meldung, sondern auch ungebetene Gäste – und genau diesen Umstand machen sich Tools wie der Network Stumbler, Aerosol oder Kismet zunutze. Diese Programme suchen gezielt nach diesen Datenpaketen und werten die darin transportierten Informationen aus.

Eine Information bei der Auswertung durch diese Tools ist für War-Driver besonders interessant: die Service Set Identifier (SSID) – besser gesagt: der Name eines Funknetzwerkes. Entwickelt wurde die SSID ursprünglich nur als logische Strukturierung, falls sich einmal die Funkwellen mehrerer Netzwerke überlappen sollten.

KNOW-HOW

So arbeiten War-Driver

Um W-LANs aufzuspüren, sind einige technische Voraussetzungen erforderlich: War-Driver brauchen eine W-LAN-Karte, die von gängigen War-Driver-Tools wie Network Stumbler, Kismet oder Aerosol unterstützt wird. Optimal dafür ist eine Karte mit dem Prism2-Chipsatz. Dieser ermöglicht es, die Karte in den so genannten Monitor-Modus zu versetzen.

Daten abhören **Damit lassen sich Daten, die über das W-LAN versendet werden, abhören. Ein ebenso wichtiger Punkt ist die Reichweite: Häufig kommen War-Driver nicht nahe genug an ihr Ziel heran oder der Weg ist durch andere Hindernisse versperrt. Zwar bieten einige Hersteller integrierte Antennen in ihren Karten an, doch beträgt deren Reichweite maximal 500 Meter.**

Externe Antennen **War-Driver arbeiten daher gerne mit externen Antennen, etwa kleinen Rundstrahlerantennen ab etwa 50 Euro. Sie erweitern den Funkbereich um bis zu einen Kilometer. Nach dem Aktivieren der W-LAN-Karte starten die Hacker den Network Stumbler. Sobald der ein W-LAN findet, erscheint im rechten Fenster unter dem Menüpunkt „MAC“ ein farbiger Kreis, der je nach Signalqualität seine Farbe ändert. Dazu zeigt das Tool die Signalstärke auch noch akustisch an. Ist im Kreis kein Schloss zu sehen, ist dies ein Indiz dafür, dass die Funkdaten unverschlüsselt übertragen werden.**

SSID preisgegeben **Unter „SSID“ verrät der Network Stumbler den Service Set Identifier, also den Netzwerknamen des gefundenen Access Points. Der muss in die Netzwerkeigenschaften der W-LAN-Karte eingetragen werden, um auf das W-LAN zugreifen zu können. In diesem Einstellungsmenü gelangt man mit einem Rechtsklick auf die Netzwerkverbindung und dann auf Eigenschaften. Nachdem die SSID in die Netzwerkeigenschaften eingetragen ist, sollte die Verbindung zum Netzwerk stehen. Ist der Access Point aber so konfiguriert, dass DHCP deaktiviert ist, vergibt er keine IP-Adresse. Somit ist ein unmittelbarer Zugang zum Netzwerk noch nicht möglich.**

WinDHCP einsetzen **In so einem Fall setzt der Hacker ein Tool wie WinDHCP ein, das die zum Netzwerk passenden IP-Adressen generiert und so den Zugriff auf das W-LAN ermöglicht. Die ausgegebene IP-Adresse muss dann zusammen mit dem Gateway in die Eigenschaften der TCP/IP-Verbindung eingetragen werden. Der Gateway ist wichtig, da sonst kein Zugriff auf das Internet möglich ist. Nun steht die Verbindung mit dem W-LAN und der Zugriff auf Ressourcen wie Freigaben und Internetzugang ist möglich.**

Die besten Sicherheits-Tipps im Web

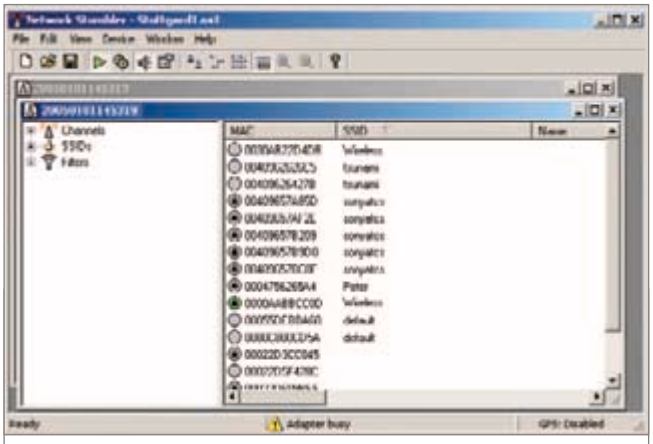
Hacker-Zentralorgan → www.wardriving.com
News, Links und Informationen für War-Driver
Hotspot-Verzeichnis → http://mobileaccess.de/wlan/
Auflistung aller bekannten bundesweiten Hotspots
Schweizer Szene → www.wireless-bern.ch
Infos zu War-Driving und Wireless Security
Standard-SSIDs bekannter Hersteller → www.cirt.net
Default-Daten zahlreicher W-LAN-Geräte

Ein Verbindungsaufbau wird vom W-LAN nur dann gestattet, wenn der anmeldende Client die gleiche SSID wie das Netzwerk vorweisen kann. Fabrikneue Access Points werden in der Regel mit Standard-SSIDs ausgeliefert. Cisco beispielsweise verwendet „tsunami", Netgear „wireless" und D-Link „wlan". Die SSIDs anderer Hersteller publiziert das Portal **www.cirt.net** unter dem Punkt „Default Wireless SSID".

Findet ein Angreifer Netzwerke mit solchen Default-Bezeichnungen, ist ihm schnell klar, von welchem Hersteller der Access Point stammt. Mit dieser Information kann er sich nun in aller Ruhe erst einmal die Handbücher auf dessen Internet-Seiten besorgen, um sich mit der verwendeten Firmware vertraut zu machen. Selbst wenn weiterführende Sicherheitsmaßnahmen wie WEP, WPA oder ACL in WLAN eingesetzt werden, zeugt eine Default-SSID nicht unbedingt von einem hohem Sicherheitsverständnis des Betreibers und lockt daher potenzielle Angreifer geradezu magisch an.

Sie sollten die Broadcast-Funktion Ihres Gerätes daher unbedingt deaktivieren. Zwar hat das den Nachteil, dass ein Verbindungsaufbau dann nur noch über eine manuelle Eingabe der erforderlichen SSID möglich ist, dafür wird das W-LAN mit dieser Maßnahme für War-Driver-Tools quasi unsichtbar gemacht. Angreifer auf der Suche nach unsicheren W-LANs können also an dieser Stelle kein Netz identifizieren und kommen daher gar nicht erst auf die Idee, einen Angriff zu starten.

Oft ist dieses Sicherheitsfeature wegen des hohen administrativen Aufwands in großen Unternehmens-Netzen mit vielen W-LAN-Clients nicht praktikabel und zudem hält es nur vorbeistreifende War-Driver ab. Da die SSID im Header an jedes Daten-Paket angehängt wird, muss sich der potenzielle Angreifer lediglich mit einem Sniffer in der näheren Umgebung postieren und auf ausgehende Funkdaten warten, um den verwendeten Wert zu ermitteln. Daher sollten Sie einige wichtige Dinge im Umgang mit der SSID beachten:



UNTERWEGS MIT NETWORK STUMBLER: Viele User verwenden trotz der Gefahren immer noch die Standard-SSID.

Verändern Sie die SSID als weitere Hürde für einen potenziellen Angreifer gleich bei der Inbetriebnahme Ihres Access Points. Es empfiehlt sich, diese Funktion als Zugangskontrolle für das W-LAN zu sehen und sie wie ein Passwort zu behandeln. Bezeichnungen wie „firma-xy.buchhaltung.untergeschoss" sollten Sie vermeiden, weil damit dem Hacker die Orientierung innerhalb des Funknetzes maßgeblich erleichtert wird und er durch die Preisgabe der zu erwartenden Inhalte wahrscheinlich nur noch stärker angelockt wird.

Verwenden Sie eine möglichst lange Kombination aus Buchstaben, Ziffern und Sonderzeichen. Nutzen Sie die Groß- und Kleinschreibung und gebrauchen Sie keine Wörter, die im Lexikon stehen, da diese mit so genannten Wortlisten leicht geknackt werden können. Eine SSID wie 1yXq34*$56hrZvWdA78eE0 Oijl2 schützt nicht nur vor dem Kompromittieren der SSID durch primitive Brute-Force-Attacken, sondern bietet noch eine weitere entscheidende Schutzfunktion vor einem anderen Angriff: Programme wie WEPCrack sammeln zum Entschlüsseln von WEP die versendeten Pakete des W-LAN-Netzwerkes. Da aber zum Beispiel der Wi-Fi-Treiber von Linux keine Checksummenprüfung der Daten vornimmt und die Sonderzeichen in der SSID, die ja in jedem Paket enthalten sind, für das Programm nicht lesbar sind, werden sie als defekte Pakete deklariert und verworfen. Mit anderen Worten: Damit können keine verschlüsselten Pakete des W-LANs gesammelt beziehungsweise geknackt werden.

Einfache Standard-Passwörter

Ist das W-LAN erst einmal aufgespürt, wird ein Angreifer im Regelfall unverzüglich mit unterschiedlichen Methoden versuchen, auf das Internet oder im LAN verfügbare Systeme zuzugreifen. Häufig ist dies wegen der Access-Point-Konfiguration nicht möglich, weil beispielsweise DHCP deaktiviert wurde. Um sich eine langwierige Suche nach der „richtigen" IP-Adresse zu ersparen, untersuchen viele War-Driver zunächst den Access Point auf Schwachstellen.

Dessen Einrichtung und Administration erfolgt in der Regel via SNMP-Manager (Simple Network Management Protokol), der mit dem entsprechendem Treiber des Access Points auf der Internet-Seite des Herstellers erhältlich ist und per USB-Verbindung oder bequem über den Browser per Web-Interface ausgeführt werden kann. Um einen Missbrauch zu vermeiden, erfolgt die Anmeldung an das Konfigurationsmenü über die Abfrage eines Benutzernamens und eines Passwortes. Werkseitig ist der Zugang zum Gerät jedoch lediglich durch ein vom Hersteller ausgewähltes Standardpasswort gesichert. Die Firma Netgear verwendet zum Beispiel das nicht sehr originelle Passwort „password", und Cisco „schützt" das Gerät mit dem eigenen Firmennamen. Allzu oft verzichtet man auf ein Sicherheitsfeature, das den User nach der ersten Anmeldung zwingt, ein neues Passwort zu setzen. Daher vergessen viele ungeübte Anwender bei der Konfiguration diesen Schritt. →

Gibt es Probleme beim Zugriff, testet der War-Driver zunächst die Integrität des gesetzten Passworts. Tools wie Network Stumbler oder Aerosol verfügen über eine integrierte Datenbank sämtlicher Hersteller- und Produktnamen, mit der diese Programme die Informationen aus den aufgefangenen Daten-Paketen abgleichen können. Ist der Hersteller bekannt, reicht ein Griff zum Handbuch oder auf die Support-Seite des Unternehmens, um neben den üblichen Produkthinweisen auch das jeweils verwendete Standardpasswort des Geräts herauszufinden.

Bei weit verbreiteten Access Points genügt meist ein Blick auf eine der zahlreichen War-Driver-Passwort-Datenbanken, beispielsweise unter **www.cirt.net**.

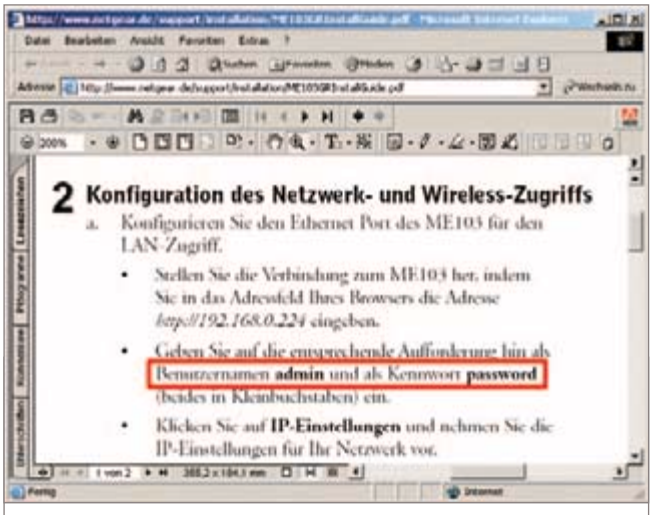
Doch selbst wenn das Passwort im Laufe der Installation bereits geändert wurde, ist das für die wenigsten Hacker in der näheren Umgebung ein Grund zur Resignation, denn mit Hilfe so genannter Brute-Force Angriffe, zum Beispiel mit dem Passwort-Cracker Brutus, ist das Knacken von Trivial-Passwörtern, die lediglich aus Buchstaben mit weniger als 6 Zeichen bestehen, in kurzer Zeit möglich.

Ist der Zugriff erfolgreich verlaufen, kann der Angreifer nun damit beginnen, die Konfigurationen und Einstellungen des Access Points zu manipulieren und seinen Zugriff auf das angeschlossene LAN oder auf darin befindliche Systeme auszubauen.

Hacker nutzen Bugs in der Firmware

Doch selbst wenn auch ein solcher Angriff scheitern sollte, ist der Hacker noch nicht am Ende. Mit Hilfe der bisher gesammelten Informationen kann er weiterführende Maßnahmen gegen den Access Point vorbereiten. Dazu muss er lediglich die einschlägigen Bug-Listen, etwa **www.securityfocus.com**, nach Schwachstellen des Geräts durchforsten. Oft genug lassen sich Fehler in der Firmware des Systems ermitteln, mit denen es möglich ist, Sicherheitsmaßnahmen zu umgehen. Damit lässt sich ein unter Umständen ein langwieriges Knacken von Passwörtern oder Schlüsseln vermeiden.

Unverständlicherweise reagieren einige Geräte mit einem Reset beziehungsweise dem Verwerfen von Konfigurationseinstellungen auf so genannte Denial-of-Service-Attacken (DoS).


2 Konfiguration des Netzwerk- und Wireless-Zugriffs
a. Konfigurieren Sie den Ethernet Port des ME103 für den LAN-Zugriff.
• Stellen Sie die Verbindung zum ME103 her, indem Sie in das Adressfeld Ihres Browsers die Adresse http://192.168.0.224 eingeben.
• Geben Sie auf die entsprechende Aufforderung hin als Benutzernamen admin und als Kennwort password (beides in Kleinbuchstaben) ein.
• Klicken Sie auf IP-Einstellungen und nehmen Sie die IP-Einstellungen für Ihr Netzwerk vor.

STATT PASSWORT-CRACKING: Ein Blick ins Online-Handbuch genügt, um die Standard-Passwörter herauszufinden.

Cisco warnte beispielsweise vor einem Fehler in der IOS-Firmware des AP1100, 1200 und 1400, über den ein Angreifer mit Hilfe einer manipulierten Anfrage an den Webserver des Konfigurationsmenüs einen Reboot erzwingen kann, ohne dazu vorher eine Authentifizierung zu benötigen.

Andere Systeme, zum Beispiel der W-LAN-Access-Point WG602v1 von Netgear, haben einige ihrer Firmware-Versionen mit Master-Passwörtern ausgestattet, die durch ein Informationsleck beim Hersteller oder von findigen Hackern ausfindig gemacht wurden. In diesem Fall lautet der Benutzername „super“, und als Passwort dient die Telefonnummer eines Zulieferers aus Taiwan: 5777364.

Fehlerhafte Versionen der internen Geräte-Software lassen sich durch ein Update der Firmware korrigieren. Informieren Sie sich daher regelmäßig, ob Firmware-Updates verfügbar sind und spielen Sie diese ein, um fehlerbereinigte Versionen der internen Geräte-Software zu erhalten.

Doch nicht alle Geräte bieten die Möglichkeit, ein Update der Firmware durchzuführen. Besonders bei preisgünstigen „No-Name“-Produkten ist dies oft gar nicht vorgesehen. Aus Kostengründen hat man bei diesen Geräten auf ausgefeilte Sicherheitsfeatures verzichtet und damit ist Ihnen ein Mitwachsen mit den Anforderungen, beispielsweise neue Sicherheitsfeatures, das Betreiben mit einem neuem Betriebssystem oder das Beseitigen von Bugs, durch das Aufspielen einer neuen Firmware-Version verwehrt. Informieren Sie sich daher vor dem Kauf eines Access Points über die Möglichkeit eines Firmware-Updates.

Sniffing – Lauschangriff aufs W-LAN

Wie schon erwähnt, ist das Abhören, das so genannte Sniffing, eine der größten Gefahren im W-LAN. Dabei sind Wireless-Netzwerke, die ihre Daten unverschlüsselt übertragen, besonders anfällig für Sniffing-Attacken. Der Hacker muss lediglich zur richtigen Zeit zur Stelle sein, um die über das W-LAN im Klartext gesendeten Daten, beispielsweise Passwörter, Zugangsdaten, bedeutsame Dokumente, persönliche Daten oder wichtige Dateien, abzufangen.

Die Gefahr des „Sniffens“ von Funkdaten geht an dieser Stelle weniger von patroullierenden War-Drivern aus; vielmehr werden diese Angriffe eher von Hackern oder neugierigen Nachbarn in der unmittelbaren Umgebung Ihres W-LAN-Standortes gestartet. Denn je nach Höhe des jeweiligen Datenaufkommens können diese Angriffe unter Umständen recht langwierig sein, sodass Hacker viel Geduld mitbringen müssen. Weiterhin ist das richtige Timing wichtig für den Angreifer; schließlich muss er zur Stelle sein, sobald sensible Daten das Funknetz passieren.

Momentan ist das Sniffen in städtischen Zentren oder an Universitäten und Fachhochschulen, wo es zahlreiche Hotspots gibt, sehr beliebt. Denn um den Anwendern einen besonders einfachen und bequemen Zugang ins W-LAN zu ermöglichen, verzichten einige Betreiber trotz der bekannten Sicherheitsrisiken auf jede Verschlüsselung. Die meisten User dieser Hotspots ahnen wahrscheinlich überhaupt nicht, dass beim Abrufen ihrer E-Mails oder beim Einloggen auf einem Web-Interface ihre Daten als „plain text“ (im Klartext) übertragen werden. Das bedeutet, dass jeder Teilnehmer des Hotspots die

DER EXPERTEN-TIPP

Wireless LANs wirkungsvoll absichern

Sowohl das Übertragungsmedium, also die Funkfrequenzen, als auch die Basisstation (der Access Point) und die Clients, etwa PDAs oder Notebooks, können jederzeit zum Ziel von Hacker-Angriffen werden.

Der Wirkungsbereich des Angriffs ist im Falle eines Funknetzes zunächst relativ eingeschränkt. So hat der zurzeit am Markt verfügbare Wireless-LAN-Standard 802.11g eine Reichweite von etwa 100 Metern. Durch den Einsatz von Richtfunkantennen kann die Reichweite jedoch nach Belieben erhöht werden. Zudem lassen sich Angriffe auf Funknetze kaum nachvollziehen, was die Risikobereitschaft von Angreifern steigert.

Wichtig für einen kontrollierten Funkverkehr sind Position und Reichweite des Access Points. Er sollte so aufgestellt und konfiguriert werden, dass er lediglich einen eindeutig spezifizierten Bereich mit Funkwellen versorgt. Zudem sollte der Access Point nicht in der Nähe einer Außenwand oder eines Fensters installiert werden oder mit Richt-/Patch-Antennen in seinen Abstrahlungseigenschaften eingeschränkt werden.

Die standardmäßigen Sicherheitseinstellungen von W-LANs, etwa Filtern von MAC-Adressen, Ändern der Netzwerk-ID (SSID) oder WEP-Verschlüsselung reichen nicht aus, um ein sicheres Funknetzwerk zu betreiben. Privatpersonen können sich durch Einsatz des aktuellen WPA-Standards (WiFi Protected Access) mit einem festen, nicht zu simpel gewählten Passwort (Pre-Shared Key) angemessen schützen.

Unternehmen sind dagegen gut beraten, wenn sie ein ganzheitliches Sicherheitskonzept aufsetzen, das mit den Sicherheitsmaßnahmen für das Kabel-Netz, etwa Firewalls, VPNs und Intrusion Detection-Systeme, so weit wie möglich kompatibel sein sollte. Wichtig ist, dass die Access Points keine direkte Anbindung an das lokale Netzwerk besitzen, sondern eine Firewall – etwa in Form eines W-LAN-Gateways – überbrücken müssen. Jeder Datenverkehr im Funknetz sollte nach Möglichkeit stark verschlüsselt werden. Wichtig ist auch eine starke Benutzer-Authentisierung, etwa über den Einsatz von Token Cards oder digitalen Zertifikaten. Und nicht zuletzt sollten je nach Sicherheitsanspruch des Unternehmens ständige Kontrollen durch Wireless Intrusion Detection erfolgen.

CHIP EXPERTE

Andreas Bröhl studierte Informatik an der Universität Bonn und ist seit mehr als zehn Jahren im IT-Security-Bereich tätig. Bröhl ist Leiter des Bereichs Systems Security Services bei der Firma Integralis und Chef des Integralis Tiger Team.

Integralis gilt als Europas marktführender IT-Security-Dienstleister.

→ www.integralis.de

Möglichkeit hat, Passwörter anderer Nutzer mit Hilfe eines W-LAN-Sniffers abzuhören.

So arbeiten die W-LAN-Sniffer

Im Gegensatz zu den physikalisch, also mit Kabel, miteinander verbundenen Netzen, in denen es immer noch notwendig ist, sich entweder lokalen oder Remote-Zugriff auf ein System zu verschaffen, um interne Netzwerkdaten abfangen zu können, muss sich der Angreifer beim Sniffen im W-LAN lediglich in die Nähe eines beliebigen Funknetzwerkes begeben. Um den Lauschangriff zu starten, wird die Netzwerkkarte durch den Angreifer in den so genannten „Monitor Mode“ versetzt. Im „Monitor Mode“ ist ein vollständig passives Mithören möglich, ohne selbst ein einziges Paket ins W-LAN zu senden, geschweige denn sich am belauschten Netzwerk anmelden zu müssen. Genau diese Tatsache macht das Sniffen von Funkdaten bei Hackern so beliebt.

Passiert nun ein durch den Access Point oder ein anderes im W-LAN befindliches System versendetes Paket die Netzwerkschnittstelle des Hackers, wird es von der Netzwerkkarte automatisch aufgefangen.

Eigentlich war dieser Modus bei der Ratifizierung des IEEE-802.11-Wireless-Standards überhaupt nicht vorgesehen, vielmehr diente er einigen Herstellern als Testmodus zu Debugging-Zwecken und zur Fehleranalyse. Dennoch integrierten verschiedene Unternehmen dieses Feature in die Chipsätze einiger W-LAN-Karten, darunter beispielsweise auch Prism2 und Hermes.

Sollten Sie also beabsichtigen, die Abhörsicherheit Ihres WLAN zu überprüfen, achten Sie darauf, ob Ihre Karte über einen dieser Chipsätze verfügt. Eine gute Wahl sind die Karten der Firma Orinoco oder Cisco (Aironet-Reihe). Neben der richtigen Karte benötigt der Angreifer noch ein geeignetes Tool, das den abgehörten Datenverkehr analysiert und wiedergibt. Sehr beliebt ist beispielsweise der kostenlose Open-Source-Sniffer Ethereal, mit dessen Hilfe sich einzelne Pakete verschiedener Protokolle analysieren lassen.

Besonders interessant ist für den Angreifer dabei jede Art von Passwörtern. Die werden beispielsweise bei der Anmeldung an Mail-Konten oder bei Logins auf anderen Systemen im Klartext über das W-LAN versendet und können so ohne weiteres von jedem im W-LAN befindlichen Sniffer mitgelesen werden.

Weiterhin verfügt Ethereal über eine Funktion, die es über Filterbefehle ermöglicht, Daten nur von einzelnen im Netzwerk befindlichen Clients oder Access Points abzufangen und beispielsweise „uninteressante“ Protokolle herauszufiltern. Dieses Feature des W-LAN-Sniffers ist für den Angreifer ziemlich wichtig, um in der Informationsflut nicht den Überblick zu verlieren.

Auch die ACL schützt nicht vor W-LAN-Sniffing

Beim Sniffen des Datenstromes werden auch MAC-Adressen der Geräte unverschlüsselt übertragen, und so gelingt es dem Abhörenden unter anderem, auch gültige MAC-Adressen für das Netzwerk zu erhalten. Mit verschiedenen Tools ist es möglich, die MAC-Adresse umzuschreiben, um dem Access Point ein Gerät mit einer für das Netzwerk gültigen MAC-Adresse vorzuspiegeln. Mit der so ausgerüsteten MAC-Adresse lässt sich die in der Konfiguration des Access-Points hinterlegte Access Control List (ACL) umgehen und auch dieser Schutz aushebeln.

WEP – Schutz mit Schwachstellen

Um die zu übertragenden Daten vor unbefugtem Zugriff zu schützen und auch deren Integrität sicherzustellen, hat das →

Institute of Electrical and Electronic Engineers (IEEE) ein spezielles Verschlüsselungsverfahren entwickelt, das Wired Equivalent Privacy (WEP). Es ist einer der wichtigsten Sicherheitsmechanismen von W-LAN und wurde herstellerübergreifend seit 1998 in alle Wireless-Standards integriert.

Zwar ist WEP in letzter Zeit durch das Bekanntwerden teilweise gravierender Sicherheitslücken stark ins Gerede gekommen, dennoch ist sein Einsatz eine sehr wirkungsvolle Maßnahme, um einen Großteil von Angriffen auf ein Wireless Netzwerk schon im Ansatz vereiteln zu können. Denn um WEP zu kompromittieren, benötigt ein Angreifer sehr viel Zeit, Geduld und Know-how.

Als Verschlüsselungsmethode wird bei WEP eine so genannte Stream-Chipers-Verschlüsselung eingesetzt, bei der die einzelnen Daten Bit für Bit verschlüsselt werden. Je nach vorhandener Hardware kann eine Schlüssellänge (WEP-Key) von 64 bis 256 Bit verwendet werden. Der Schlüssel setzt sich aus dem Initialisierungsvektor, einer zufälligen Zahl, die sich bei jedem Datenpaket ändert und 24 Bit lang ist, sowie dem restlichen Schlüssel in der Länge von 40 bis zu 232 Bit, der vom Anwender durch die Eingabe von WEP-Keys festgelegt wird, zusammen. Beim WEP-Verschlüsselungsverfahren beschränkt sich die Verschlüsselung auf die „Nutz"-Daten, die in einem Datenpaket versendet werden; der IP-Header selbst wird dabei also nicht verschlüsselt. Bei der Verschlüsselung wird von den „Nutz"-Daten eine Prüfsumme berechnet, die an das Paket angehängt wird. Dies soll eine Manipulation Dritter während der Übertragung der Datenpakete verhindern. Die Daten werden also anhand des gemeinsamen WEP-Keys vom Access Point verschlüsselt und vom Client entschlüsselt und umgekehrt. Da für das Ver- und Entschlüsseln ein gemeinsamer, geheimer Schlüssel eingesetzt wird, müssen sowohl der Sender als auch der Empfänger diesen Schlüssel kennen.

Die Grundlage bildet immer der vom Access Point und allen mit ihm kommunizierenden Clients genutzte identische WEP-Key. Möchte ein Client mit dem drahtlosen Netzwerk Kontakt aufnehmen, fordert der Access Point ihn auf, einen spezifischen Initialisierungsvektor anzulegen, der dann mit dem vorliegenden WEP-Key kombiniert und mit einem Algorithmus verschlüsselt wird.

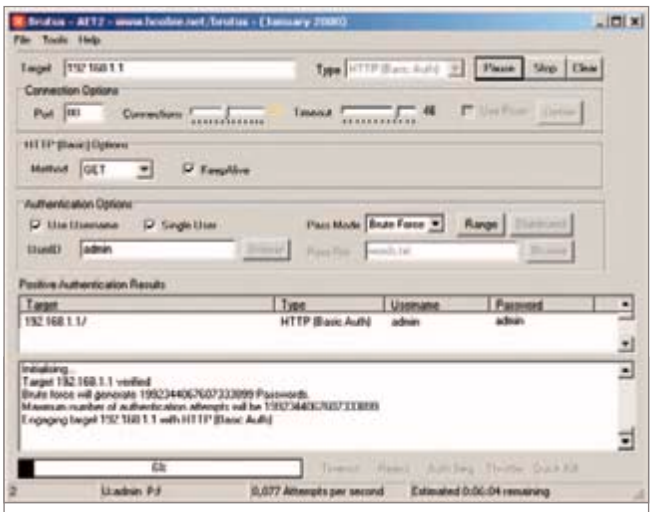
Die sicherheitslücken in WEP

Zum Erzeugen dieses Schlüssels nutzt WEP den RC4-Algorithmus. Der berechnet aus dem geheimen WEP und dem Initialisierungsvektor einen passenden Schlüssel. Und genau in diesem Verschlüsselungsalgorithmus liegt die größte Schwäche von WEP.

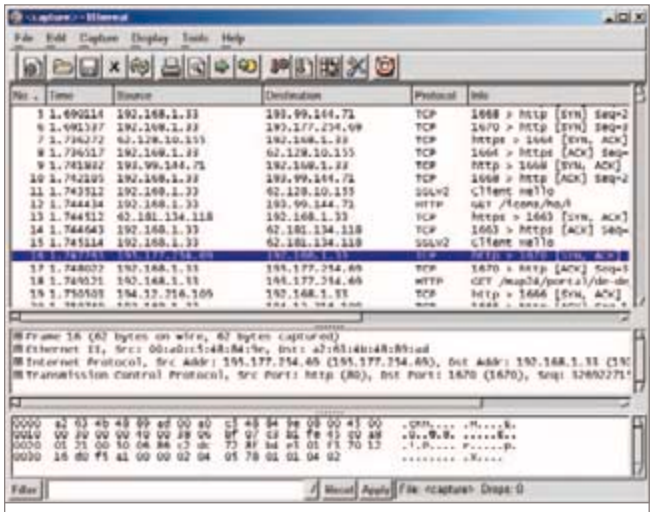
RC4 wurde 1987 von Ronald L. Rivest, einem Mitarbeiter der RSA, entwickelt. Aus Rivest's Cipher 4 wurde dann die Abkürzung RC4. Nachdem er sieben Jahre lang als streng geheim unter Verschluss lag, gelangte der Sourcecode über ein bis heute unbekanntes Sicherheitsleck in die einschlägige Cypherpunk-Mailingliste. Dadurch konnten Hacker den Algorithmus genau untersuchen, um Schwachstellen aufzudecken. Tatsächlich erkannte man schnell die Möglichkeit, die mit RC4 verschlüsselten Daten durch Umkehraktionen zu knacken. Da RC4 einige Ziffern besser als andere verschlüsselt, hat ein potenzieller Angreifer beim Empfang einer genügenden Anzahl von Paketen die Möglichkeit, den WEP-Key zu rekonstruieren.

Eine besondere Schwachstelle von WEP ist die unverschlüsselte Übertragung des Initialisierungsvektor im 802.11-Header. Daher basieren viele Angriffe auf WEP auf der Analyse des Initialisierungsvektors im Zusammenhang mit dem RC4-Output-Byte. Nun gilt es für den Angreifer, den gemeinsamen Key zu rekonstruieren. Dabei wird eine Schwachstelle beim Anlegen des nur 24 Bit langen Initialisierungsvektors, der mit einem Pseudo-Zufallsgenerator (WEP PRNG) erzeugt wird, von Tools wie WEPCrack, ausgenutzt. Bei einer Länge von 24 Bit gibt es eine begrenzte Anzahl von Kombinationen, die als Verschlüsselungsvarianten für den RC4 genutzt werden können. Bei den rund 16 Millionen möglichen Kombinationen wiederholen sich also theoretisch auch die genutzten Initialisierungsvektoren nach etwa 16 Millionen Datenpaketen.

Tools wie Airsnort benötigen in der Regel – nach Aussagen ihrer Autoren – sogar nur fünf bis zehn Millionen Pakete, um den richtigen Schlüssel zu ermitteln. Je nach Aktivität des



HÖCHST EFFEKTIV: Brute-Force-Attacken auf Access Points, bei denen ein Tool wie Brutus zahllose Anmeldeversuche startet.



ABGEHÖRT: Mit Ethereal zeichnen War-Driver unverschlüsselten W-LAN-Verkehr auf.

Clients sprechen wir an dieser Stelle von einigen Stunden, maximal von einigen Tagen. Fehlt der erforderliche Netzwerk-Traffic, kann das Angreifer-Tool die bisherigen Auswertungen speichern und seine Arbeit nach einer Unterbrechung nahtlos fortsetzen. So kann ein Hacker in der Nachbarschaft die verfügbaren Pakete über mehrere Wochen oder Monate ermitteln. Bei großen Netzwerken mit viel Traffic ist das Abfangen der entsprechend großen Anzahl auch häufig in relativ geringer Zeit möglich. Ist diese Grenze erreicht, dann ist die Ermittlung des WEP-Keys mit Hilfe eines entsprechenden Crackers nur noch eine Frage von Minuten.

Eine weitere Schwachstelle von WEP ist das fehlende Schlüsselmanagement. Da die Schlüssel in einem Netz von Hand an alle beteiligten Systeme verteilt werden müssen, führt dies in der Praxis häufig dazu, dass der Schlüssel nur sehr selten oder überhaupt nicht gewechselt wird. Diese Art und Weise der Schlüsselverteilung hat zur Folge, dass das gesamte Funknetzwerk gefährdet ist, wenn auch nur ein Schlüssel nicht geheim bleibt.

Hinzu kommt, dass sich bei der WEP-Verschlüsselung die Größe der übertragenen IP-Pakete erhöht und somit die Bandbreite der Datenübertragung innerhalb des W-LAN schmälert. Das fördert nicht gerade die Akzeptanz beziehungsweise Einsatzfreudigkeit von WEP bei Nutzern, die große Datenmengen in kurzer Zeit übertragen wollen und sich deshalb gegen die Nutzung von WEP auf Kosten der Sicherheit entscheiden. Zwar lässt sich durch den Einsatz weiterer Access Points Abhilfe schaffen. Dafür stellt sich dann wiederum die Frage der Kompatibilität der Access Points untereinander – von den damit verbundenen Mehrkosten einmal abgesehen.

Trotz all dieser Schwachstellen ist WEP nicht nutzlos, denn es ist immer noch besser als gar keine Verschlüsselung. Ihnen sollte nur klar sein, dass die WEP-Verschlüsselung nicht absolut sicher ist. Nach Bekanntwerden der genannten Schwächen im WEP und der daraus resultierenden Sicherheitsrisiken für den Anwender entschieden sich einige namhafte Hersteller zur Entwicklung alternativer Sicherungsmöglichkeiten. Doch damit diese Maßnahmen eingesetzt werden können, muss der Anwender oft auf die Hardware ein und desselben Herstellers zurückgreifen und ist somit auch bei der Erweiterung seines Netzwerkes von diesem abhängig.

WPA – die sichere Alternative

Nachdem sich WEP als relativ unsicher erwiesen hatte, zögerten viele Unternehmen, die W-LAN-Technologie einzusetzen. Andere wiederum sahen sich nach vertrauenswürdigeren Lösungen um, die als Alternativen zu WEP dienen könnten. Dadurch ergab sich für viele Hersteller die Gelegenheit, ihre eigenen Standards auf dem Markt für W-LAN-Sicherheitstechnologie zu platzieren. Doch die Flut an unterschiedlichen Protokollen macht schon heute die Interoperabilität zwischen ähnlichen Produkten unterschiedlicher Hersteller zu einem sehr großen Problem.

Daher verabschiedete das IEEE Anfang 2004 einen neuen Sicherheits- und Verschlüsselungsstandard mit der Bezeichnung Wi-Fi Protected Access (WPA), der die Lage entscheidend ändern und die grundlegenden Design-Schwächen von WEP beseitigen soll.

Im Gegensatz zur WEP-Verschlüsselung schützt WPA die Daten durch einen dynamischen Schlüssel, genauer gesagt durch vier unterschiedliche Schlüssel für jeden W-LAN-Client, der nur bei der Authentifizierung am W-LAN zum Einsatz kommt und anschließend durch einen Session-Key ersetzt wird. Die neue Schlüsselverwaltung von WPA ist ideal für große Wireless-Netzwerke, wie sie in Unternehmen zum Einsatz kommen. Mit Hilfe eines Authentifizierungs-Servers lassen sich die Zugangskennungen vom Nutzer zentral verwalten. Für kleinere, private W-LANs ermöglicht die Pre-Shared-Key-Authentifizierungsmethode, dass sich alle Teilnehmer eines Netzes mit demselben Kennwort anmelden können.

Kleine Schönheitsfehler in WPA

Doch auch in WPA wurden bereits mehrere Schwachstellen gefunden. Zwar beruhen einige davon nur auf wenig praxistauglichen Theorien und sind bei weitem nicht so gravierend wie die von WEP, dennoch gibt es besonders beim Schlüsselmanagement einiges zu beachten.

Vor allem der Group-Key, der allen Stationen bekannt sein muss, ist die Achillesferse von WPA. Ist der nämlich einer nicht autorisierten Person zugänglich, ist diese in der Lage, den anfänglichen Schlüsselaustausch zwischen Client und Access Point zu belauschen.

Eine andere Schwachstelle von WPA ist die Verwendung von zu kurzen oder leicht zu erratenden Passwörtern durch den Anwender. An dieser Stelle kann einem Angreifer unter Umständen eine Ermittlung des Passwortes gelingen.

Die Sicherheit hängt also sehr stark von der Qualität des jeweiligen Passwortes ab. Das tinyPEAP-Team (**www.tinypeap.com**) schrieb aufgrund dieser Sicherheitsproblematik ein unix-basierendes Programm namens WPA Cracker. Der Hacker muss dazu lediglich mit einem Sniffer wie Ethereal während der WPA-Authentifizierungsphase, bei der sich der User am W-LAN authentifiziert, einzelne Pakete aufzeichnen. Das Tool versucht dann entweder per Brute Force oder mit einer Wörterbuch-Attacke den während der WPA-Authentifizierung ausgetauschten Schlüssel offline zu rekonstruieren.

Ein anderes Problem von WPA haben Hacker im integrierten Message-Integrity-Check-Algorithmus gefunden, der eigentlich als Schutz vor möglichen Angreifern dienen sollte. Er wurde ursprünglich entwickelt, um Brute-Force-Attacken abzuwehren, bei denen ein Hacker mit Hilfe eines speziellen Tools das Netzwerk durch ständiges Anmelden mit verschiedenen Kennwörtern angreift. Beim Einsatz des Message-Integrity-Check-Algorithmus werden, sobald innerhalb weniger Sekunden mehr als ein falscher Schlüssel an den Access Point geschickt wird, sämtliche Verbindungen sowie der Access Point für einen gewissen Zeitraum deaktiviert. Dies ist allerdings insofern kritisch, als ein Angreifer, etwa mit einem PDA oder Handy, nur ganz wenige Pakete mit falschen Zugangsdaten schicken muss, um das System dauerhaft lahmzulegen.

Ein weiterer, nicht zu vernachlässigender Nachteil von WPA ist die höhere Rechenzeit, die aufgrund der stärkeren Verschlüsselung anfällt. Besonders bei älteren Systemen kann es daher zu Problemen mit der Performance kommen.

Thomas Vosseberg

Hacker aussperren

W-LAN perfekt abschirmen

Sicherheitsrisiken gibt es im W-LAN mehr als genug, doch Sie haben auch viele Möglichkeiten, um War-Driver oder Hacker erfolgreich abzuwehren. Gerade die Kombination der Sicherheitsmaßnahmen nimmt vielen Eindringlingen schnell die Lust, sich in Ihr W-LAN einzuschmuggeln. CHIP sagt Ihnen, wie Sie Ihr Funknetz abschotten.

Genauso wie bei der Absicherung eines herkömmlichen Kabel-Netzwerkes gilt: Hundertprozentige Sicherheit gibt es nicht. Denn dazu schreitet die technische Entwicklung zu schnell voran. Doch was man als User tun kann, das sollte man auch tun – und alle gebotenen Möglichkeiten nutzen, um einen angemessenen Schutz zu erreichen.

Die Devise lautet: Mach es dem Hacker so schwer wie möglich! Baue möglichst viele Hürden ein. Je mehr Arbeitsschritte ein Angreifer absolvieren muss und je mehr Zeit ihn das kostet, um so weniger reizvoll wird die Attacke für ihn, und er wird sich in den meisten Fällen ein einfacheres Ziel suchen. Sie sollten darüber hinaus regelmäßig Ihre Benutzerkennungen und Passwörter ändern, die Sicherheitsmeldungen der Hersteller beachten sowie einschlägige Publikationen lesen, um auf dem neuesten Stand zu bleiben. Denn was heute als besonders sicher gilt, ist morgen schon veraltet. Doch dafür gibt es dann in der Regel schon wieder etwas Besseres…

Dieser Beitrag zeigt Ihnen, wie Sie Ihr drahtloses Netzwerk so sicher wie möglich machen, um ungebetene Gäste auszusperren.

Sicherheitsstufen kombinieren

In der Regel hilft dabei die relativ einfache Kombination der mitgelieferten Sicherheitsfeatures, beispielsweise:

Abschalten von Broadcast-Funktion und DHCP

Verschlüsseln der Daten mit WEP

WPA beziehungsweise den noch besser verschlüsselten Wi-Fi-Standard WPA2, entsprechend dem IEEE-Standard 802.11i, aktivieren

Authentifizierung der einzelnen Clients mit Hilfe der Access Control List (ACL) über die MAC-Adressen der Clients.

Zwar bringt jede dieser Maßnahmen ihre spezifischen Schwachstellen mit sich, für deren Ausnutzung oft genug eine ganze Reihe von frei verfügbaren Tools im Internet erhältlich sind. Dennoch steht der hohe Arbeits- und Zeitaufwand, den der Angreifer zum Überwinden dieser Hürden investieren muss, in keinem Verhältnis zum Resultat.

CHIP → DVD-CODE W-LAN, Security

- **Alle Tools** Auf Heft-DVD finden Sie die passenden Tools (Code: W-LAN), etwa AirSnare, Airopeek SE, Network Stumbler, Kismet, Aerosol, Airsnort, WEPCrack und Ethereal.
- **Sicherheit** Schützen Sie Ihr W-LAN mit den besten Gratis-Antiviren-Tools und -Firewalls, wie AntiVir PE, AVG Anti-Virus Free und ZoneAlarm (DVD-Code: Security).

Wenn irgend möglich, sollten Sie die Basisstation nur dann einschalten, wenn sie auch tatsächlich benötigt wird. Schließen Sie das Gerät am besten über eine Steckdosenleiste mit Schalter an das Stromnetz an.

Verschlüsselung verstärken

Aufgrund der recht späten Veröffentlichung der Sicherheitslücken in WEP war es für eine Lösung des Problems längst zu spät, da der Verschlüsselungsstandard bereits in Millionen von 802.11-Geräten zum Einsatz kommt.

Dennoch ist es mit einigen einfachen Schritten für jeden möglich, WEP robuster zu machen. Bei der Anschaffung eines Wireless-Gerätes sollten Sie unbedingt darauf achten, dass es die maximale Schlüssellänge von 128 oder sogar 256 Bit unterstützt. Beachten Sie auch, dass diese sowohl von den Netzwerkkarten als auch vom Access Point unterstützt wird.

Ändern Sie die Schlüssel in regelmäßigen Abständen. Einige Geräte, etwa die Aironet-Reihe von Cisco, unterstützen bereits eine automatische Schlüsselerneuerung. Sollte Ihr Access Point schon WPA unterstützen, aktivieren Sie es anstelle von WEP. Einige Hersteller bieten über ein Update der Firmware auch WPA für Geräte an, die bisher nur WEP-Verschlüsselung ermöglichen. Informieren Sie sich am besten auf der Webseite des Herstellers über ein entsprechendes Update.

Außerdem sollten Sie bei der Anschaffung neuer Geräte darauf achten, dass es sich dabei um so genannte RSN-Hardware handelt. „RSN“ steht für die Robust-Security-Network-Sicherheitsarchitektur, die mit dem 802.11i-Standard eingeführt wurde und die W-LAN-Sicherheit erheblich verbessert. Dabei ist das „i“ am Ende der Bezeichnung von 802.11i sehr wichtig, da bei den vorherigen Standards bis zu 802.11h zunächst mehr Wert auf die Standardisierung, die Interoperabilität und die Übertragungsgeschwindigkeit gelegt wurde. Erst mit der Weiterentwicklung durch den 802.11i-Standard trat ein umfassendes Sicherheitskonzept in den Vordergrund. Mit diesem Standard werden neue Verschlüsselungsprotokolle wie CCMP, in dem das AES-Verschlüsselungsverfahren genutzt wird, eingesetzt, beispielsweise von WPA2.

Das Sicherste ist somit der Einsatz von WPA2, da von AES variable Schlüssellängen von 128, 192 oder 256 Bit erzeugt werden. Dadurch haben Hacker kaum noch eine Chance, die so verschlüsselten Pakete zu knacken.

Eine weitere Möglichkeit der Verschlüsselung bietet das Einrichten eines Virtual Private Network (VPN). Besonders für Unternehmen mit wichtigen betriebsinternen Daten sind die bisherigen Verschlüsselungsverfahren WEP und WPA aufgrund

Die besten Sicherheits-Tipps im Web

Jede Menge Know-how → www.wardrive.net
Ausführliche Infos über Wireless Security und War-Driving
Amtshilfe → www.bsi.de/literat/doc/wlan
Tipps vom Bundesamt für Sicherheit in der Informationstechnik
Viele Praxisartikel → www.monolith81.de/wirelesslan
Artikel und Workshops zum Thema Wireless-Sicherheit
Hacking-Security → www.sub7.de
Umfangreiches IT-Sicherheitsboard mit W-LAN-Forum

der hinlänglich bekannten Sicherheitsprobleme nicht akzeptabel. Wegen des vereinfachten Schlüsselmanagements von VPN hält sich der damit verbundene Verwaltungsaufwand auch bei einer Vielzahl von Clients in Grenzen. In Kombination mit einem Sicherheitszertifikat und zusammen mit der Standardverschlüsselung von VPN lässt sich somit ein Maximum an Sicherheit erreichen.

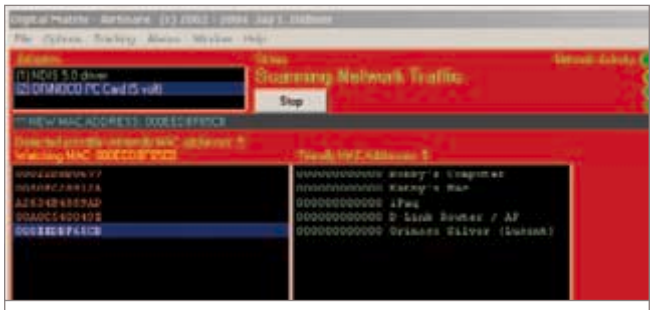
Weiterhin sollten Sie bei der drahtlosen Übertragung wichtiger Daten, zum Beispiel bei der Anmeldung an Ihrem Mail-Account, SSL verwenden. Dadurch werden die Daten zwischen Ihrem Computer und dem Server verschlüsselt. Niemand dazwischen kann diese Daten einfach auslesen. Einige Mail-Provider bieten dies bereits für ihre diversen Kommunikationsprotokolle, beispielsweise IMAP, POP3 und SMTP, an. Informieren Sie sich dazu am besten auf der Homepage Ihres Internet-Providers. Beachten Sie, dass auch beim Surfen im Internet SSL eingeschaltet ist, wenn Sie persönliche Daten austauschen. Dass SSL aktiv ist, erkennen Sie daran, dass in Ihrem Browser rechts unten in der Anschlussleiste ein kleines Schloss erscheint (Zugriffsmöglichkeit etwa im Internet Explorer über „Extras | Internetoptionen | Erweitert"). Verzichten Sie beispielsweise lieber auf einen drahtlosen Einkauf über das Internet, wenn der Server des Shops kein SSL benutzt. Denken Sie daran, dass Ihre persönlichen Daten andernfalls jederzeit in die Hände unbefugter Dritter fallen könnten.

W-LAN überwachen

Um einen unberechtigten Zugriff auf ein W-LAN aufzudecken, bieten einige Access Points eine Funktion zum Anlegen von Log-Dateien. An dieser Stelle kann sich der Anwender darüber informieren, welche Clients sich am Wireless-Netzwerk angemeldet haben – aber auch unerwünschte Zugriffe kommen dabei ans Tageslicht. Allerdings ist dies erst dann möglich, wenn der Angriff bereits erfolgt ist und der Hacker sich eventuell schon weit ins lokale Netzwerk beziehungsweise auf andere Clients vorgearbeitet hat.

Programme wie das Windows-basierende Intrusion Detection System (IDS) AirSnare oder Airopeek von WildPackets bieten daher die Möglichkeit, sämtliche Aktivitäten in einem W-LAN genau zu analysieren und Alarm zu schlagen, bevor bleibende Schäden entstehen. Bei diesen Programmen handelt es sich in der Regel um spezielle Sniffer-Tools, die den gesamten Netzwerkverkehr penibel auf verdächtige Aktivitäten und Signaturen überprüfen.

So lässt sich beispielsweise in Echtzeit feststellen, ob unberechtigte Clients angemeldet sind, unerlaubte Access Points im



INTRUSION DETECTION SYSTEM: Das IDS AirSnare erkennt Angreifer im W-LAN und warnt den Administrator.

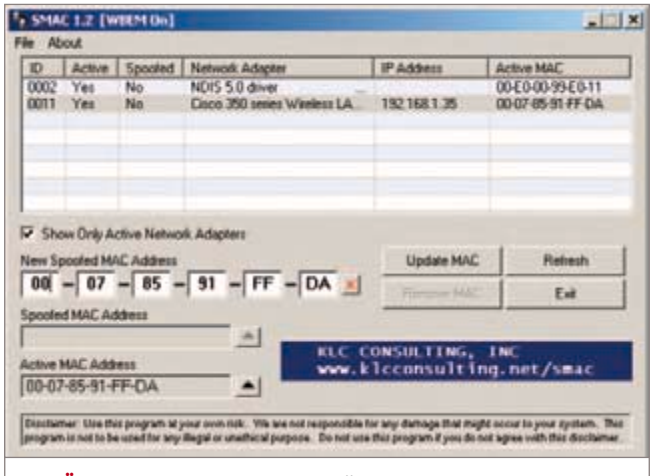
W-LAN aufgestellt wurden, oder ob jemand versucht, den Datenverkehr abzufangen. Entdeckt beispielsweise das Tool AirSnare eine neue Station im Netzwerk, deren MAC-Adresse nicht bekannt ist, protokolliert es den verursachten Traffic und schickt per Mail eine Warnmeldung an den Netzwerk-Administrator, damit der umgehend auf die drohende Gefahr reagieren kann.

W-LAN durch Firewall absichern

Immer mehr Access Points verfügen bereits über eine interne Firewall. Besitzt auch Ihr Access Point eine Firewall, sollten Sie sie aktivieren und die Konfiguration während der Einrichtung noch einmal genau überprüfen.

Neben den Standard-Sicherheitsmaßnahmen, die über den Access Point gesteuert werden, sollte auch das Netzwerk beziehungsweise dessen Clients vor Attacken geschützt werden. Ist es nämlich einem Angreifer bereits gelungen, die Firewall des Access Points zu durchbrechen, stehen ihm in der Regel sämtliche Systeme im lokalen Netz weit offen.

Im kleinen W-LAN reicht schon der Einsatz einer Desktop-Firewall wie Zone Alarm. Bei größeren Netzwerken ist die Basisstation am besten hinter einer Hardware-Firewall postiert. Außerdem sollten Sie dringend auf die Systemsicherheit Ihrer Clients achten. Installieren Sie beispielsweise immer einen aktuellen Virenscanner, um das Einschleusen von Schädlingen in das System zu verhindern. Zudem sollten Sie regelmäßig Up- →


SMAC 1.2 [WBEM On]
File About
ID Active Spoofed Network Adapter IP Address Active MAC
0002 Yes No NDIS 5.0 driver 00-E0-00-99-E0-11
0011 Yes No Cisco 350 series Wireless LA... 192.168.1.35 00-07-85-91-FF-DA
Show Only Active Network Adapters
New Spoofed MAC Address
00 - 07 - 85 - 91 - FF - DA
Update MAC
Refresh
Exit
Spoofed MAC Address
Active MAC Address
00-07-85-91-FF-DA
KLC CONSULTING, INC
www.klcconsulting.net/smac

MAC ÄNDERN: Das Tool SMAC ermöglicht es, die MAC-Adresse unter Windows per Mausklick zu verändern.

dates und Patches für Betriebsystem und Software einspielen. Nur so kann auch hier optimale Sicherheit erreicht werden.

Der W-LAN-Penetrationstest

Nach erfolgreicher Inbetriebnahme und Abschirmung des Funknetzes sollten Sie die Sicherheit Ihres Netzwerks selbst gründlich testen, um auszuschließen, dass Ihnen bei der Konfiguration Fehler unterlaufen sind. Der Umstand, dass die Clients Kontakt zur Basisstation haben, bedeutet nicht das automatische, ordnungsgemäße Greifen aller Sicherheitsmechanismen. Dazu sollten Sie sich erst einmal mit den Werkzeugen eines Angreifers vertraut machen. Laden Sie sich etwa die entsprechenden Tools wie Network Stumbler, Kismet, Aerosol, AirSnort oder WEPCrack von der Heft-DVD.

Das eigene Netz angreifen

Versetzen Sie sich dazu zunächst in die Lage eines vorbeifahrenden War-Drivers, der versucht, Ihr Netzwerk aufzuspüren. Dazu verwenden Sie am besten den Network Stumbler oder Aerosol. Finden die Programme Ihre Basisstation, sollten Sie das SSID-Broadcasting unbedingt ausschalten.

Um die Verschlüsselung zu testen, setzen Sie einen Sniffer wie Ethereal ein, um gerade ausgetauschte Daten abzuhören. Nach dem Auswerten der aufgefangenen Daten überprüfen Sie, ob die Verschlüsselung ordnungsgemäß arbeitet. Melden Sie sich dazu am besten mit einem anderen „regulär" im W-LAN befindlichen Client an einer Netzwerk-Freigabe oder einem Postfach an. Im Log des Sniffers darf keinerlei Klartext zu erkennen sein.

Kontrollieren Sie als nächstes den Sendebereich Ihrer Basisstation. Testen Sie dabei mit einer Antenne, wie stark sich Ihr W-LAN ausbreitet. Die räumliche Ausdehnung Ihres W-LAN können Sie mit Hilfe der Geräteposition und der Antennenausrichtung am Access Point in punkto Senderichtung und Reichweite beeinflussen. Falls Ihre Basisstation ein Reduzieren der Sendeleistung erlaubt, sollten Sie diese Funktion nutzen, um den Angreifern den Empfang und somit das Finden Ihres W-LAN zu erschweren.

Im zweiten Hauptschritt sollten Sie die Chancen längerer Angriffe überprüfen. Installieren Sie am besten einen separaten Client in das W-LAN, der weder über eine in der ACL zugelassene MAC-Adresse noch über einen gültigen WEP-Key verfügt.

Mit dem Programm SMAC ist es einem Angreifer möglich, die MAC-Adresse seines Systems nach Belieben zu verändern. Nun muss er lediglich versuchen, eine zugelassene MAC-Adresse, beispielsweise aus aufgefangenen Daten, zu erhalten oder sie einfach zu erraten.

MAC-Adressen herausfinden

Was im ersten Moment nur wenig erfolgversprechend klingt, hat jedoch durchaus Methode. Besonders kleine Netzwerke vergeben ihren Systemen standardmäßig IP-Adressen im Bereich zwischen 192.168.0.1 bis 192.168.2.255, da auch die meisten Netzwerkgeräte vom Hersteller aus mit Adressen in diesem Bereich ausgeliefert werden. Die Anwender behalten diese IP-Adressen gleich bei.

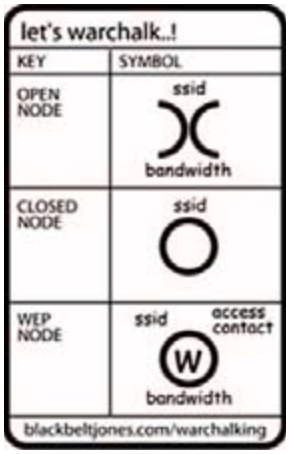
Dabei erhöhen sich die Chancen des Hackers erheblich, eine gültige MAC-Adresse herauszufinden, je mehr Geräte in der ACL des Access Points eingetragen und zum Zeitpunkt des Angriffs nicht im W-LAN angemeldet sind. Ist also ein Client längere Zeit nicht mehr im W-LAN, wird dessen MAC-Adresse aus der Liste gelöscht und bei Bedarf wieder eingetragen.

Verwenden Sie auch keinen Standard-IP-Adressbereich für das W-LAN, wie er im Auslieferungszustand des Access-Points festgelegt ist. Legen Sie stattdessen lieber einen höheren Wert wie etwa 192.168.20.x fest.

KNOW-HOW

Die Zeichen der War-Driver

Um andere War-Driver über ihre Erkenntnisse zu informieren, zeichnen Hacker die Spezifikationen der vorgefundenen Netzwerke an Wände und auf Bordsteine (Warchalking). Dieser Trend kommt aus Großbritannien. Dort entwarf der Grafiker Matt Jones eine Karte, auf der er die Symbole zum Markieren von W-LAN-Netzwerken festlegte. Die Idee beruht auf einer alten Tradition von Landstreichern und Trampern. Um zu signalisieren, dass es in einem bestimmten Haus Essen oder aber einen bissigen Hund gibt, zeichneten sie Symbole an Wände und Zäune.



WARCHALKING: Jetzt weiß jeder, wo Schwarzsurfen möglich ist und wo nicht.

Ähnlich verhält es sich mit den Symbolen der War-Driver. So verraten etwa zwei offene Halbkreise jedem, dass hier ein vollkommen unverschlüsseltes Netz funkt. Hintergedanke ist der Wunsch vieler W-LAN-Aktivisten nach einem flächendeckenden Internet-Zugang für jedermann. Zwar gibt es schon etliche Hotspots (öffentliche Funkzugänge, siehe etwa die Seite von Mobileaccess unter http://mobileaccess.de/wlan), doch um überall auf das Internet zuzugreifen, braucht man so viele Zugänge wie möglich. Dabei sollen die Warchalking-Zeichen helfen.

In London tauchten derart viele Zeichnungen auf, dass einige Tageszeitungen die weitgehend unwissende Bevölkerung aufklären mussten, was sie bedeuten. Das System der Mitteilungen ist sehr simpel und besteht aus nur drei Symbolen. Mit der links gezeigten Karte in der Hand ist es damit jedoch jedermann möglich, einmal aufgespürte Netzwerke zu spezifizieren und deutlich für andere War-Driver zu kennzeichnen.

Open Node Zwei gegeneinander aufgestellte Halbkreise symbolisieren einen offenen Node. An dieser Stelle befindet sich ein offenes W-LAN, das direkten Zugang ins Internet liefert und IP-Adressen per DHCP verteilt.

Closed Node Ein Kreis symbolisiert einen geschlossenen Node. An dieser Stelle befindet sich ein geschlossenes WLAN-Netzwerk, in dem entweder kein Internet-Zugang besteht oder der Online-Zugang nicht ohne weitere Aktivitäten möglich ist.

WEP Node Ein „W" in einem geschlossenen Kreis symbolisiert, dass das entdeckte Funknetzwerk die so genannte WEP-Verschlüsselung aktiviert hat. An dieser Stelle ist der Weg ins Internet erst frei, nachdem der WEP-Code geknackt ist.

DER EXPERTEN-TIPP

Unbefugte Zugriffe entdecken und abwehren

Das klassische War-Driver-Szenario kommt bei Firmen eher selten vor; es ist einfach zu auffällig. Wer im parkenden Auto sitzt und mit seinem Notebook in ein W-LAN eindringen will, hält sich eher an Privatwohnungen.

Mitarbeiter als Risiko Viel häufiger ergeben sich Sicherheitslücken durch die eigenen Mitarbeiter, oft auch unbeabsichtigt. Es kommt etwa vor, dass Mitarbeiter, die ein W-LAN zu Hause haben, einen eigenen Access Point ins Büro mitbringen, um dort Daten schneller auf mobile Geräte kopieren zu können. Solche Access Points verfügen nur äußerst selten über Sicherheitsmechanismen wie Wi-Fi Protected Access (WPA) oder eine sichere Verschlüsselung und stellen ein enormes Sicherheitsrisiko im Unternehmensnetz dar.

Fremde Hardware aufspüren Zum Aufspüren fremder Geräte oder von Eindringlingen mussten früher teure Zusatzsysteme installiert werden. Alternativ konnte der IT-Administrator persönlich mit Laptop oder Handheld und Analysesoftware durch das Gebäude laufen und danach Ausschau halten.

Ausgereifte W-LAN-Software Sie ersetzt heute diese keineswegs sicheren Methoden, denn sie kann unbefugte Zugriffe anzeigen und Eindringlinge aufspüren. Voraussetzung dafür ist ein identitätsbasierendes Anmeldesystem zur Positionsbestimmung der einzelnen Nutzer, wenn sie sich durch das Gebäude bewegen. Das System muss die zugrundeliegende Funknetz- und Netzwerk-Infrastruktur verstehen. So können Access Points in regelmäßigen „Sweeps“ alle Kanäle des W-LANs abtasten, unbefugte Zugriffe entdecken und durch Berechnungen sogar die Position des Eindringlings im System anzeigen.

Authentifizierung Ein beidseitiger Authentifizierungsprozess kann die Sicherheit des Firmen-W-LANs weiter steigern. Clients müssen bei der Anmeldung am Netzwerk eine Authentifizierung vorweisen, fordern diese aber auch von den Access Points. Wenn auch Access Points beweisen müssen, dass sie zum Firmen-W-LAN gehören, ist die Gefahr geringer, dass sich jemand an einem falschen Access Point anmeldet.

Vorbeugung ist auch im Wireless LAN die beste Verteidigung: Die 802.1X-Authentifizierung kombiniert mit 802.11i-Verschlüsselung oder sogar die Vorgänger dieses Standards wie WPA schützen sensible Unternehmensdaten nachhaltig.

CHIP EXPERTE

Michael Coci ist Product Marketing and Support Director für EMEA bei Trapeze Networks.

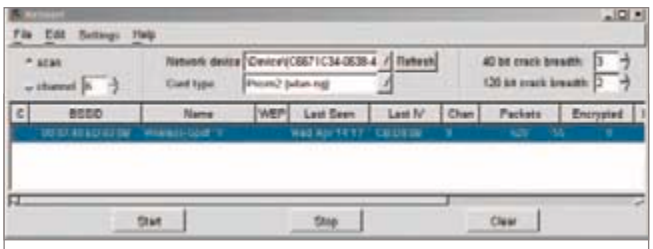
Das kalifornische Unternehmen bietet leistungsstarke Business-Anwendungen und -Dienstleistungen für die mobile Belegschaft von Firmen.

→ www.trapezenetworks.com

Um die Verschlüsselung zu testen, benötigen Sie ein Tool wie AirSnort oder WEPCrack. Diese Programme können WEP-Keys aus dem laufenden Netzwerkverkehr herausfiltern und entschlüsseln. Dazu brauchen sie lediglich die Gelegenheit, genügend verschlüsselte Pakete zu protokollieren.

Diese Programme laufen ausschließlich mit Netzwerkkarten, die über einen Prism2-Chipsatz oder einen gepatchten Treiber verfügen und sich in den Monitor-Mode versetzen lassen, etwa Orinoco oder Cisco Aironet. Zwar werden die meisten WEP-Cracker ausschließlich unter Linux genutzt, doch mit AirSnort haben auch Windows-User die Möglichkeit, WEP zu entschlüsseln. Für die Installation von AirSnort auf Windows müssen Sie zusätzlich noch GLIB und GTK+1.3 installieren, unter Linux ist es ähnlich. Doch wenn die Karte erst einmal unter Linux läuft, wird sie mit an Sicherheit grenzender Wahrscheinlichkeit auch mit AirSnort problemlos zusammenarbeiten.

Nun müssen Sie das Programm nur noch starten, und der Angriff kann beginnen. Laut Beschreibung benötigt es dazu etwa fünf bis zehn Millionen Datenpakete, die mit demselben Key verschlüsselt sind, um genügend Informationen für das Entschlüsseln eines schwachen Algorithmus herauszufiltern. In der Praxis sind es mehr als doppelt so viele, doch im Gegensatz zu einem potenziellen Angreifer müssen Sie nicht darauf warten, bis diese über den normalen Netzwerkverkehr abgearbeitet werden. Das Sammeln der Informationen dürfte ansonsten mehrere Tage dauern. Kopieren Sie einfach größere Datenmengen über das W-LAN von einem Client zu einem anderen und lassen Sie AirSnort nebenbei sniffen. Nach einigen Stunden sollte feststehen, wie sicher Ihr Schlüssel wirklich oder ob Sie Ihr Schlüsselmanagement nicht noch einmal überdenken sollten. In jedem Fall sollten Sie wenigstens vier Schlüssel verwenden und sie mindestens einmal im Monat ändern. Damit machen Sie es einem Angreifer noch schwerer, denn wenn ein Schlüssel geknackt worden ist, muss er seine Arbeit von neuem beginnen.



WEP CRACKEN: **AirSnort sammelt schwach verschlüsselte Pakete und ermittelt daraus WEP-Keys.**

Für das Knacken von WPA brauchen Sie zwar weit weniger Pakete, doch genauso viel Geduld wie ein richtiger Hacker, denn dabei handelt es sich um eine Offline-Attacke. Ein Sniffer wie Ethereal zeichnet lediglich die WPA-Authentifizierungsphase auf, und danach wird das W-LAN mit einem WPA-Cracker einer Brute-Force-Attacke unterzogen. Je nach Länge des Pairwise Master Key, also des Passworts, und je nach Performance des jeweiligen Prozessors kann dies unter Umständen wochenlang dauern. Daher sollten Sie auch an dieser Stelle das Passwort in regelmäßigen Abständen ändern.

Am Ball bleiben

Geht man mit der neuen Technologie richtig um, kann diese genauso sicher sein wie die bereits eingesetzte. Dies ist aber nur möglich, wenn Sie nicht nur die eben kennengelernten Werkzeuge regelmäßig einsetzen, sondern am Ball bleiben und Ihr Wissen auf dem neuesten Stand halten.

Thomas Vosseberg

Zehn Tipps: W-LAN absichern

Ihre Nachbarn surfen – und Sie zahlen die Zeche

War-Driver gelten als gefährliche Hacker. Eine viel größere Gefahr stellt jedoch oft der Büronachbar dar: Will er in Ihr Funknetz einbrechen, steht ihm die Tür meist weit offen. Denn kaum ein W-LAN-Betreiber verschlüsselt seine Funkdaten. CHIP zeigt, wie Sie Ihr Netzwerk sichern und alte W-LAN-Hardware updaten.

Stehen Sie schon auf der Liste? Schauen Sie nach: In Datenbanken wie unter **www.artchalking.com** speichern W-LAN-Knacker ihre Erfolgsmeldungen und alle Informationen zu ihren letzten Raubzügen. Geben Sie einfach Ihre Postleitzahl ein. Steht Ihr Straßenname dort? Der Name Ihres Funknetzwerks? Dann sollten Sie schneller lesen! Denn in diesem Artikel erklärt CHIP, wie Sie Ihr W-LAN vor unerwünschten Mitsurfern absichern, es mit neuester Verschlüsselungstechnik uneinnehmbar machen und nur die Computer mitfunken lassen, die Ihnen gehören.

Die große Gefahr für das Funknetz geht in den meisten Fällen nicht von bösen War-Drivern aus, die systematisch Straße für Straße abfahren, um ungeschützte W-LANs zu enttarnen. Viel wahrscheinlicher sitzt der Hacker in der Wohnung oder dem Büro nebenan. Der einfache Grund: Der Nachbar kann dauerhaft von Ihrem offenen W-LAN profitieren. Zudem bekommt er eher ein Funksignal von Ihrem Router, weil er sich näher an der W-LAN-Quelle befindet. Und wenn Ihr Funknetz eine Verbindung zum Internet besitzt, freut sich der Nachbar erst richtig – über billiges Surfen auf Ihre Kosten.

Das Sicherheitsproblem von W-LANs besteht darin, dass Funknetzwerke einfach zu installieren sind. Ist der W-LAN-Router erst einmal eingeschaltet, sendet er regelmäßig die Kennung „Ich bin das Netzwerk mit dem Namen ‚default'" und wartet auf Kundschaft. Die Funknetzkarte im Notebook muss nur noch diese Meldung aufschnappen, schon steht die Verbindung – sogar die in allen Netzwerken notwendige IP-Adresse bekommt das Notebook vom Router. Mit den folgenden zehn Tipps schotten Sie Ihr Funknetz zuverlässig ab.

TIPP 1 | W-LAN-Router sicher starten

Verbinden Sie Ihren W-LAN-Router bei der ersten Konfiguration per Netzwerkkabel mit dem PC. Das ist erstens bequemer, und zweitens können keine ungesicherten Funkdaten bei der Konfiguration herausgehen.

→ Schalten Sie erst den W-LAN-Router ein und danach den PC. Der Router ist nämlich in der Regel auch der DHCP-Server in Ihrem Netzwerk. Startet der PC nach dem Router, dann erhält er automatisch eine IP-Adresse.

→ Öffnen Sie einen Web-Browser und geben Sie die IP-Adresse des Routers ein (steht im Handbuch). Dort finden Sie auch das vom Hersteller vorab vergebene Admin-Kennwort für den W-LAN-Router.

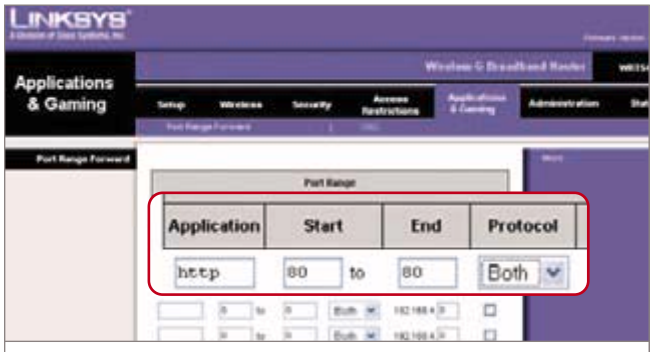
→ Ändern Sie dieses Admin-Kennwort sofort, denn Listen mit diesen Standard-Passwörtern findet jeder angehende Hacker im Web. Meist steht die entsprechende Option unter „Administration | Admin-Settings" oder in der „Basiskonfiguration". Achtung: Mit dem Zugriffskennwort sichern Sie lediglich den Router vor Manipulationen, nicht die Funkverbindung!

→ Schalten Sie die Verschlüsselung für das Funknetz ein. Verwenden Sie nach Möglichkeit die WPA-Verschlüsselung mit einem Preshared Key. In den Optionen finden Sie diese Einstellung unter einem Kürzel wie „WPA-PKS". Geben Sie zusätzlich ein sicheres Kennwort ein, das aus Buchstaben, Ziffern und Sonderzeichen bestehen sollte.

Falls Sie den W-LAN-Router über ein Funknetz konfiguriert haben, geht nach dem Speichern der Verschlüsselungskonfiguration zunächst die Verbindung verloren. Öffnen Sie dann die Software für Ihre W-LAN-Karte im PC, wählen Sie das Verschlüsselungsverfahren und geben Sie das Kennwort ein.

TIPP 2 | WEP-Verschlüsselung nutzen

Der gängigste Weg, ein Funknetz abzusichern, ist die Verschlüsselung der zu übertragenden Daten. Außenstehende bekommen so nichts vom Funkverkehr mit und können sich ohne Kennwort nicht einklinken. Der verbreitete Verschlüsselungsstandard WEP (Wired Equivalent Privacy), der in den meisten Funknetzen eingesetzt wird, weist allerdings Schwachstellen auf.



1 | PORT FORWARDING: In den Router-Optionen lassen sich einzelne Ports freigeben und an PCs im LAN weiterleiten.

Ein per WEP übertragenes Datenpaket setzt sich zusammen aus einem so genannten Initialisierungsvektor (IV) und den verschlüsselten Daten. Die enthalten ihrerseits noch eine Check-Summe, um Manipulationen an den Daten aufzudecken.

Hauptschwachpunkt von WEP ist der Initialisierungsvektor. Er ist immer 24 Bit lang. Aus ihm und dem WEP-Schlüssel errechnet ein Algorithmus den verschlüsselten Code, der per Funk übertragen wird. Aus dem dabei im Original übertragenen IV und dem WEP-Schlüssel ermittelt die Gegenstelle anschließend die Original-Daten.

Das Problem: Zwar empfiehlt der WEP-Standard, dass jedes übertragene Paket einen anderen Initialisierungsvektor haben sollte. Aber erstens hält sich nicht jeder Hersteller daran, und zweitens steht nirgends, wie der IV erzeugt wird. Meist wird ein Pseudo-Zufallsgenerator genutzt. Die Folge: Früher oder später wiederholt sich der IV. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rechnet damit, dass nach etwa 4.000 versandten Datenpaketen ein identischer IV auftaucht, die Universität von Berkeley glaubt an eine Wiederholung des IV nach 5.000 Paketen. Fängt ein Hacker zwei Datenpakete mit identischem Initialisierungsvektor ab, kann er den WEP-Schlüssel ermitteln – und schon haben Sie einen ungebetenen Gast im Netz. Der kann Daten mitschneiden, sich beim Access-Provider anmelden oder sogar Check-Summen fälschen und damit Daten manipulieren. Dafür braucht ein Angreifer nicht einmal teure Software. Programme, die WEP knacken, gibt es kostenlos im Internet, etwa unter **http://wepcrack.sourceforge.net** oder **http://airsnort.shmoo.com**.

TIPP 3 | Das Risiko WEP minimieren

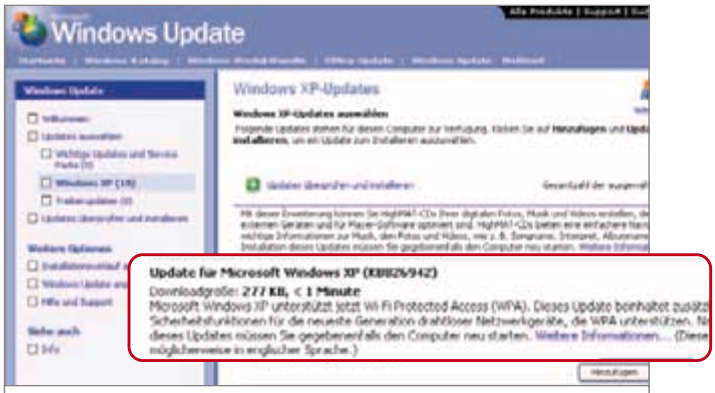
Besonders einfach haben es Angreifer, wenn für die Verschlüsselung nur 40 Bit lange Schlüssel verwendet werden (64 Bit minus 24 Bit IV). Denn die sind so kurz, dass man die möglichen Kombinationen einfach durchprobieren kann und innerhalb kurzer Zeit den Code geknackt hat. Da die Schlüssel meist nur sehr selten gewechselt werden, lohnt dieser Aufwand für Angreifer. Danach steht das Funknetz für lange Zeit offen. Falls Sie also WEP nutzen, schalten Sie zumindest die Verschlüsselung mit 104 Bit ein (128 Bit minus 24 Bit IV).

TIPP 4 | WPA statt WEP einsetzen

Wer wirklich sicher sein möchte, sollte den neuen Standard WPA (Wifi Protected Access) wählen, der das Protokoll TKIP (Temporal Key Integrity Protocol) verwendet. Der Trick: Zu Beginn der Übertragung vereinbaren beide Funkstationen einen individuellen Start-Schlüssel. Dafür muss das eigentliche Kennwort nur einmal übertragen werden. Ausgehend vom Start-Schlüssel erhält jedes übertragene Datenpaket einen individuellen Key zur Verschlüsselung. Bei diesem Verfahren ist es fast unmöglich, an den Original-Code zu kommen. Der Nachteil: WPA kostet mehr Rechenzeit und erzeugt einen größeren Daten-Overhead, Sie können also nicht so schnell funken wie mit WEP.

TIPP 5 | Die Hardware sicher machen

Bei W-LAN-Routern führt der Weg zu WPA nur über ein Firmware-Upgrade. W-LAN-Adapter für den PC brauchen neue, WPA-kompatible Treiber (jeweils auf der Hersteller-Homepage).



5 | NEUE SICHERHEIT: Installieren Sie das WPA-Update für Windows XP, um das Funknetz besser zu sichern.

Auch Windows XP braucht eine Auffrischung, damit es WPA unterstützt. In jedem Fall muss das Service Pack 1 installiert sein. Dazu kommt ein Patch mit dem Namen „Windows XP-Supportpatch für Wireless Protected Access". Den finden Sie über das Windows-Update (**http://windowsupdate.microsoft.com**) in der Rubrik „Windows". Weitere Informationen zu diesem →

PORT FORWARDING

Online-Spiele via Router nutzen

Manchmal muss man das sorgsam geknüpfte Sicherheitsnetz ein wenig öffnen, etwa um einen eigenen Webserver zu betreiben oder zum Spielen von Online-Games. Denn solche Dienste benötigen spezielle Ports, die von der Firewall normalerweise gesperrt werden.

Das Zauberwort, um dennoch durch die Firewall zu kommen, heißt „Port Forwarding". In Ihrem Router finden Sie dazu, meist unter dem Eintrag „Firewall" oder „Security", eine Option namens „Port Settings". Falls nicht, sehen Sie nach unter Menüpunkten wie „Applications" oder „Applications & Gaming". Dort können Sie einen einzelnen Port oder einen ganzen Port-Bereich freischalten. Daten aus dem Internet, die an diesen Ports ankommen, werden dann direkt an einen Computer in Ihrem lokalen Netzwerk weitergeleitet.

Ein Port lässt sich allerdings immer nur einem lokalen PC zuweisen. Falls also mehrere Computer in Ihrem Netz Filesharing betreiben wollen, brauchen Sie in der Filesharing-Software eine Option, um den normalerweise verwendeten Port zu ändern.

Achtung! Mit jeder Port-Freigabe schaffen Sie eine Sicherheitslücke in Ihrem Netzwerk und einen weiteren möglichen Angriffspunkt.

Mit der Port Address Translation (PAT) und der Network Address Translation (NAT) hat das Port Forwarding übrigens nichts zu tun. Bei NAT sorgt der Router wie ein Vermittler dafür,

→ dass ein PC aus Ihrem lokalen Netzwerk im Internet mit der öffentlichen IP-Adresse des Routers auftritt und

→ dass Ihr Router die aus dem Internet zurückkommenden Daten an den richtigen LAN-Computer weiterleitet.

PAT erweitert dieses Verfahren mit einem Trick auf mehrere Computer im lokalen Netzwerk: Jeder lokale PC, der Daten aus dem Internet anfordert, erhält vom Router einen spezifischen Port zugewiesen, an den der Internet-Server seine Daten schickt. Anhand dieser Port-Nummer weiß der Router dann automatisch, an welchen lokalen Computer er die Daten weiterleiten muss.

Patch liefert Microsoft unter der URL **http://support.microsoft.com/?kbid=826942**.

Nach der Installation des Patches finden Sie in den Eigenschaften der Netzwerkverbindung unter „Drahtlose Netzwerke“ die SSID Ihres Netzwerks. Mit einem Klick auf „Konfigurieren“ gelangen Sie in ein weiteres Menü, in dem Sie als „Netzwerkauthentifizierung“ den Eintrag „WPA-PSK“ wählen. Möglicherweise steht dort auch eine andere Bezeichnung, sie sollte aber in jedem Fall auf „WPA“ und „Pre-Shared Key“ schließen lassen. Ansonsten fehlt Ihnen der aktuelle Treiber.

TIPP 6 | Notfalls lieber mit WEP verschlüsseln

Falls es mit WPA nicht klappt, gilt: Besser schwach verschlüsseln als gar nicht. Schalten Sie also in jedem Fall die WEP-Verschlüsselung ein und nutzen Sie die maximale Schlüssellänge. So verhindern Sie zumindest, dass sich jemand einfach so in Ihr Netz einklinkt. Für den Schlüssel verwenden Sie einen Code aus Hexadezimal-Zeichen. Der bietet mehr Variationsmöglichkeiten als ein Schlüssel, der nur aus Buchstaben oder Zahlen besteht. Wechseln Sie den Schlüssel regelmäßig.

TIPP 7 | SSID verschleiern

Falls Ihr W-LAN-Router eine Option besitzt, die Funknetz-Kennung (SSID) zu verschleiern, sollten Sie diese einschalten. Zusätzlich müssen Sie den Namen des Netzwerks ändern – denn die meisten Funknetze heißen „default“. Wählen Sie stattdessen eine nicht nahe liegende Bezeichnung, keinesfalls den Familien- oder Firmennamen. Denn ist die SSID versteckt, muss der Hacker diese Bezeichnung von Hand eingeben – das wirkt wie ein Kennwort. Allerdings bringt dieser Trick allein keine absolute Sicherheit, denn Tools wie Network Stumbler → **Heft-DVD** spüren auch versteckte Funknetze auf.

TIPP 8 | MAC-Adressen filtern

Als weitere Sicherheitsmaßnahme gegen unbefugte Eindringlinge sollten Sie nur bestimmte MAC-Adressen für das Netzwerk zulassen. MAC-Adressen sind 48 Bit lange Kennungen für Netzwerk-Adapter – wie eine Personalausweis-Nummer. Die Einstellungen in Ihrem W-LAN-Router finden Sie meist unter einem Stichwort wie „MAC-Filter“. Dort tragen Sie die MAC-Adressen Ihrer Clients in eine Liste ein. Manche W-LAN-Router erlauben sogar, die Adressen der aktuell angemeldeten Clients in die Liste zu übernehmen. Falls nicht, bekommen Sie die MAC-Adresse Ihres Funknetz-Adapters über die Windows-Kommandozeile („Start | Ausführen… | cmd“) mit der Eingabe von „ipconfig/all“ heraus. Der Schwachpunkt: MAC-Adressen lassen sich fälschen.

PROFI-TIPP

Web-Schutz deaktivieren

Wer das Risiko liebt oder eine Software nutzt, die nicht über eine Firewall betrieben werden kann, darf einen PC im lokalen Netz als DMZ einrichten – in der so genannten „Demilitarisierten Zone“. Dieser unglücklich gewählte Begriff bezeichnet einen Computer, der komplett gegenüber dem Internet geöffnet wird. Die im W-LAN-Router eingebaute Firewall schützt diesen Computer dann nicht mehr!

Die Option zum Freischalten finden Sie im Router in den Firewall-Einstellungen unter „DMZ“ oder „Demilitarized Zone“. Dort geben Sie die IP-Adresse Ihres Computers ein.

Achtung: Wenn Sie einen frisch installierten Windows-PC ohne Sicherheits-Updates in der DMZ freigeben, wird er mit hoher Wahrscheinlichkeit innerhalb weniger Sekunden Opfer eines Wurm-Angriffs.

TIPP 9 | DHCP abschalten

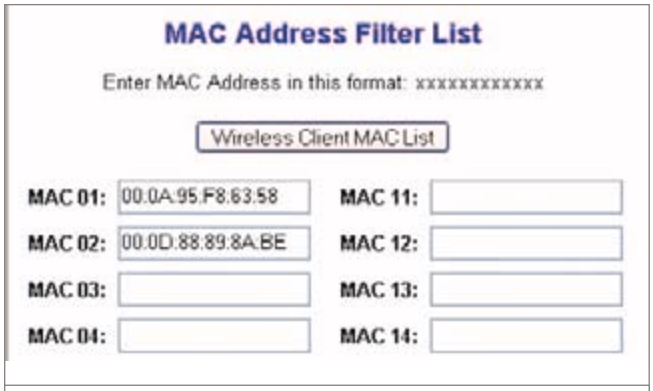
Auch das Abschalten des DHCP-Servers in Ihrem W-LAN-Router zählt zu den Sicherheitsmaßnahmen. Denn der weist jedem Neuankömmling im Netz automatisch eine IP-Adresse zu. Verwenden Sie stattdessen statische IP-Adressen, die Sie jedem Client einzeln verpassen. Zusätzliche Sicherheit bringt es, statt der üblichen 192.168.0.1 weniger übliche IP-Adressen zu nutzen, zum Beispiel 192.168.167.1.

TIPP 10 | Sicherheitsmaßnahmen kombinieren

Wer nur WEP verwendet, sollte in jedem Fall auch die MAC-Filterung einschalten und die SSID seines Funknetzes verschleiern. So wird das W-LAN halbwegs sicher. Wirklich ruhig schlafen kann aber nur, wer statt WEP das weitaus stärkere WPA verwendet, am besten in Kombination mit den anderen Sicherungen. Die Arbeit für das Upgrade von Windows und der Treiber lohnen sich.

Martin Goldmann

5 | SCHLÜSSELDIENST: In den „Drahtlosen Netzwerkeigenschaften“ schalten Sie den WPA-Verschlüsselungsmodus ein.



8 | SICHERHEITSPLUS: Der MAC-Adressen-Filter regelt, welche W-LAN-Adapter sich an Ihrem Router anmelden dürfen.

Recht: Ungebetene Gäste im Netz

Schwarzsurfer im W-LAN

Die Versuchung ist groß, denn auf Schritt und Tritt sind sie zu finden – ungeschützte W-LANs, die geradezu zum Schwarzsurfen einladen. Was kaum einer weiß: In vielen Fällen handeln die ungebetenen Gäste noch nicht einmal strafbar, sondern nutzen eine juristische Grauzone.

Es ist so einfach: Mit dem Auto in Schrittgeschwindigkeit durch ein Wohngebiet fahren – das eingeschaltete Notebook, das offene Funknetze akustisch meldet, liegt griffbereitauf dem Beifahrersitz. Wenn's piept, parkt der Fahrer unauffällig am Straßenrand und geht über das nächste ungeschützte W-LAN ins Internet, um mal eben kostenlos neue Mails abzurufen oder auch Dateien herunterzuladen.

Dass es tatsächlich ein Spaziergang ist, in fremde W-LANs einzubrechen, liegt vor allem an der teilweise unglaublichen Sorglosigkeit der Anwender: Untersuchungen haben ergeben, dass jedes zweite Funknetz in Deutschland ungeschützt ist. Zahlreiche Anwender machen sich nicht einmal die Mühe, nach dem Einrichten eines W-LAN-Routers den voreingestellten Netzwerknamen (SSID) zu ändern, geschweige denn die WEP- oder WPA-Verschlüsselung zu aktivieren (mehr dazu lesen Sie im Sicherheits-Special ab 68).

Gelegenheit macht Diebe, heißt es, doch im Fall der W-LAN-Einbrüche ist es noch keineswegs ausgemacht, dass überhaupt ein strafbares Verhalten vorliegt. Ist „Mit-Surfen" strafbar, wenn dem Betreiber – dank Flatrate – gar kein finanzieller Schaden entsteht? Ist der Betreiber des Funknetzes für einen eventuell erlittenen Schaden selbst verantwortlich, wenn er sein W-LAN nicht gesichert hat?

Diese und andere brisante Fragen zum Thema „W-LAN-Einbrüche" beantwortet Ihnen dieser Artikel.

Erlaubt: Absichtlich offengehaltene W-LANs nutzen

Wer ein Funknetz nicht gegen „unberechtigtes" Eindringen besonders sichert, kann meist keine rechtlichen Ansprüche oder Sanktionen herleiten. Denn ein W-LAN-Betreiber, der willentlich sein Funknetz nicht schützt, nimmt es offensichtlich in Kauf, dass er für den Traffic anderer (Schwarz-)Surfer aufkommen muss. Und wenn er eine Flatrate nutzt, was unter Internet-Anwendern immer häufiger der Fall ist, entsteht dem W-LAN-Betreiber auch kein finanzieller Schaden. Der Schwarzsurfer, der zusätzlichen Traffic verursacht, macht sich also grundsätzlich nicht strafbar.

Allerdings darf der offene Internet-Zugang zu nichts anderem als zum kostenlosen Surfen genutzt werden. Wenn der Eindringling beispielsweise Schäden durch das Ausspähen, Verändern oder Zerstören von Daten verursacht, muss er durchaus mit rechtlichen Konsequenzen rechnen.

Straflos: Versehentlich offene W-LANs nutzen

Vorsicht: Beileibe nicht jedes offene Funknetz wurde vom Betreiber mit Absicht offengehalten. Zwar könnte der W-LAN-Knacker im Streitfall argumentieren, dass bei unabsichtlich offengehaltenen Netzwerken zumindest der Anschein dafür spricht, dass der Funknetz-Betreiber mit der Fremdnutzung durch Schwarzsurfer einverstanden ist, da er andernfalls sein W-LAN geschlossen und gesichert hätte.

Diesem Anschein könnte der Netzwerk-Betreiber mit dem Argument entgegentreten, dass ihm die technischen Kenntnisse für das Einrichten eines wirkungsvollen Schutzes fehlen. Der Schwarzsurfer kann nicht stillschweigend davon ausgehen, dass er das fremde W-LAN nutzen darf. Dabei gilt der Grundsatz, dass Unwissenheit nicht vor Strafe schützt. Zudem werden die Gerichte davon ausgehen, dass sich der Schwarzsurfer durchaus bewusst ist, dass er fremde Ressourcen nutzt.

Letztendlich wird es aber auch in diesem Fall an einem Schaden beziehungsweise einem erfüllten Straftatbestand fehlen.

Verboten: In gesicherte W-LANs eindringen

Wer noch dreister ist und bewusst in ein geschlossenes, also gesichertes Funknetz eindringt, verhält sich dagegen rechtswidrig. Das gilt besonders, wenn der ungebetene Gast nicht nur surft, sondern auch noch fremde Daten ausspäht, sie verändert oder gar zerstört.

Fazit: Rechtswidrig, aber meist straffrei

Zumindest das Eindringen in W-LANs, die mit WEP oder WPA besonders gegen unbefugte Zugriffe gesichert sind, kann strafbar sein. Ein Hacker, der etwa durch die unberechtigte Verwendung eines WEP-Schlüssels in ein Funknetz eindringt, kann den Straftatbestand des „Computerbetrugs" erfüllen und riskiert eine Freiheitsstrafe von bis zu fünf Jahren oder eine Geldstrafe.

Dagegen bleibt das Nutzen fremder W-LANs zum kostenlosen Internet-Surfen straflos – allerdings nur, wenn keine Verschlüsselung umgangen wird und der Eindringling keine Schäden am Datenbestand des betroffenen W-LANs verursacht. Straflos heißt aber nicht kostenlos. Denn W-LAN-Betreiber, die nachweisen können, durch einen Schwarzsurfer materiell geschädigt worden zu sein – beispielsweise durch überhöhte Provider-Kosten –, können unter Umständen zivilrechtliche Schadenersatzansprüche stellen.

W-LAN-Knacker bewegen sich derzeit in einer rechtlichen Grauzone und müssen in bestimmten Fällen mit strafrechtlichen Konsequenzen rechnen – insbesondere wenn sie in geschützte Funknetze eindringen. Ob ein paar auf Kosten anderer eingesparte Euro Providerkosten dieses Risiko rechtfertigen, muss jeder Schwarzsurfer selbst entscheiden.

Michael Schweizer, Andreas Vogelsang

PRAXIS | INHALT

Filme & Musik per W-LAN 84
Ein Rechner reicht als Quelle: So schicken Sie große Multimedia-Dateien per Funk durch die Wohnung.

Kameraüberwachung 92
Keine Angst vor Einbrechern: Per W-LAN lassen sich Grundstücke und Gebäude bequem überwachen.

Site Survey: Richtig planen 96
Wer ein professionelles W-LAN aufbauen will, sollte zuvor das Funkareal auf Störeinflüsse prüfen.

Professionelle Hotspots 102
Wer mit funkenden PC-Freunden Geld verdienen will, erfährt hier alles über Profi-Hotspots.

Weg mit dem Festnetz 110
Mit W-LAN lässt sich eine Festnetzleitung bequem ersetzen. Sicherheit ist aber höchstes Gebot.

Mesh-Netze per W-LAN 114
Multi-Hop- oder vollvermascht: Hintergründe und Grundlagen für große Wireless LANs.

Die Zigbee-Revolution 118
Experten sehen in Zigbee den Zukunftsstandard für Funknetze – CHIP erklärt, was dahinter steckt.

Netz unter Kontrolle 122
W-LANs müssen ständig kontrolliert werden – so ist die Statusabfrage am einfachsten.

Fehler schnell finden 128
Funktioniert's nicht so, wie Sie wollen? Mit diesen Schritten lassen sich Fehler schnell finden.

Schneller, besser, sicherer 134
Mit unseren Profi- und Tuning-Tipps holen Sie noch mehr aus Ihrem Wireless LAN heraus.

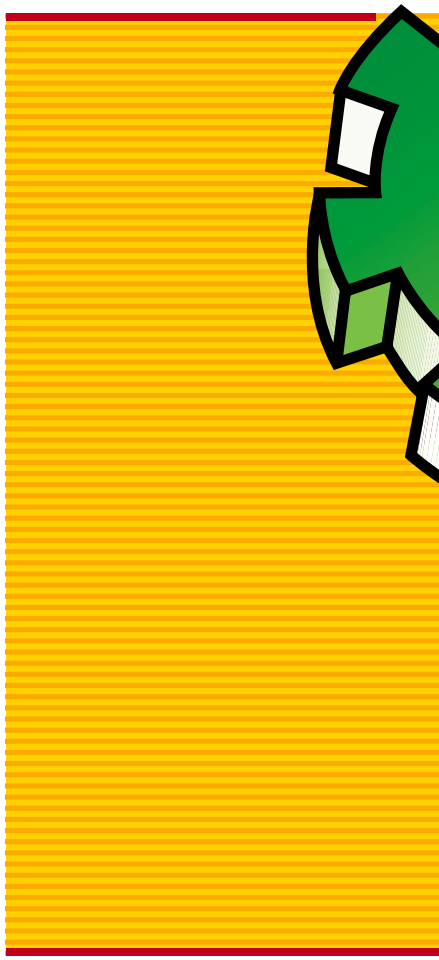
Gewusst wie! 142
Wichtige Tipps und Tricks rund um das Einrichten, Konfigurieren und Kontrollieren von W-LANs

CHIP AUTOR → www.srg.at

Robert Schoblick ist seit 1991 freier Journalist. Er beschäftigt sich mit Themen der modernen Telekommunikations- und Informationstechnik. Gemeinsam mit seiner Frau führt der Diplom-Ingenieur der Nachrichtentechnik seit 1996 ein Redaktionsbüro und verfasste bisher mehrere hundert Fachbeiträge in renommierten Magazinen sowie mehr als zwei Dutzend Fachbücher.

CHIP → DVD-CODE Basics

- → **LAN-Player** Auf der Heft-DVD finden Sie den Gratis-Media-Player VideoLAN Client. Mit dem Tool lassen sich Multimediadaten im Netzwerk streamen.
- → **WMP im Netz** Mit Hilfe von on2share streamen auch Anwender des Windows Media Players (WMP) Sound- und Video-Dateien über das Netzwerk.



Auf der Terrasse lassen Sie sich von Ihren Lieblingshits aus dem Internet unterhalten. Dann schauen Sie sich die Urlaubsfotos im Arbeitszimmer an. Nach dem Blockbuster im Wohnzimmer noch ein Online-Spiel im Schlafzimmer – das gibt's nicht? Doch, mit einem drahtlosen Home-Entertainment-Netz.

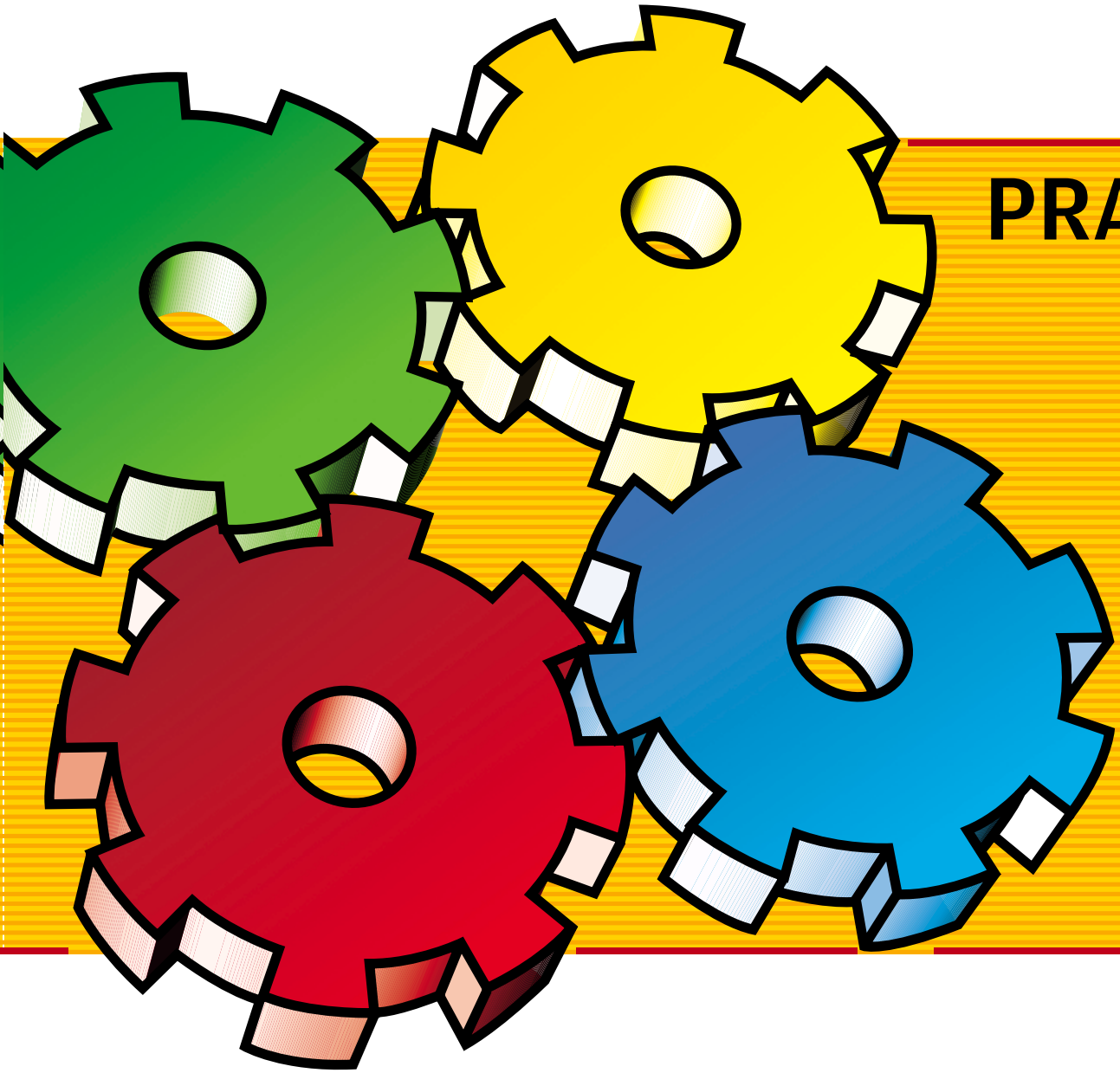
Home-Entertainment-Netz

Filme und

Heimnetze dienen immer noch hauptsächlich zum Verbinden von PCs, um Ressourcen und Internet-Anschluss gemeinsam zu nutzen. Doch das wird sich ändern. Schon bald werden auf demselben Netzwerk alle möglichen Arten von Daten – einschließlich Audio- und Videosignale – durch das ganze Haus transportiert. Mit der richtigen Hardware können Sie schon heute ein drahtloses Entertainment-Netz aufbauen.

Vier Standards konkurrieren

Musik- oder Video-Signale lassen sich auf einem leitungsgebundenen oder einem drahtlosen Netzwerk übertragen. Bei einer Kabelverbindung ist die Sicherheit am ehesten gewährleistet. Stehen die Rechner jedoch nicht im selben Zimmer, vielleicht sogar auf unterschiedlichen Etagen, offenbart die billige und leistungsstarke Kabellösung einen Nachteil: Entweder müssen die Kabel aufwendig durch die Wohnung verlegt werden oder es werden Löcher durch Wände und Decken gebohrt, um die Kabelführung möglichst kurz zu halten. Eine Alternative ist



PRAXIS

Musik per W-LAN

ein Netzwerk mit Funkverbindung; sie ist allerdings teurer und komplizierter als ein Kabelnetz. Bevor Sie sich für einen Standard entscheiden, sollten Sie die Vor- und Nachteile der einzelnen W-LAN-Techniken kennenlernen.

Vier drahtlose Standards konkurrieren derzeit um einen Sendeplatz. IEEE 802.11b („IEEE“ steht für „Institute of Electrical and Electronical Engineers“, das US-Pendant zum DIN, dem „Deutschen Institut für Normung“) ist eher für die Unternehmens-Umgebung gedacht und bietet eine gute Abdeckung von großen Büroräumen. 802.11a bietet eine größere Bandbreite und weniger Interferenz-Probleme, dafür ist die Reichweite geringer. Bluetooth ist für kurze Funkstrecken oder die vorübergehende Vernetzung von Konferenz-, Vortrags- oder Klassenräumen konzipiert.

Der jüngste Spross der drahtlosen Technologien ist 802.11g, ein Standard, der 2003 seinen amtlichen Segen erhielt. 802.11g kombiniert die große Reichweite von 802.11b mit dem hohen Datendurchsatz von 802.11a. Ein weiterer Vorteil: Die Technik ist voll kompatibel zu 802.11b. Einen Vergleich der aktuellen Standards zeigt die Tabelle unten.

802.11 g, lange als der leistungsstarke Nachfolger von 802.11b gehandelt, wurde im Juni 2003 ratifiziert, aber schon Monate →

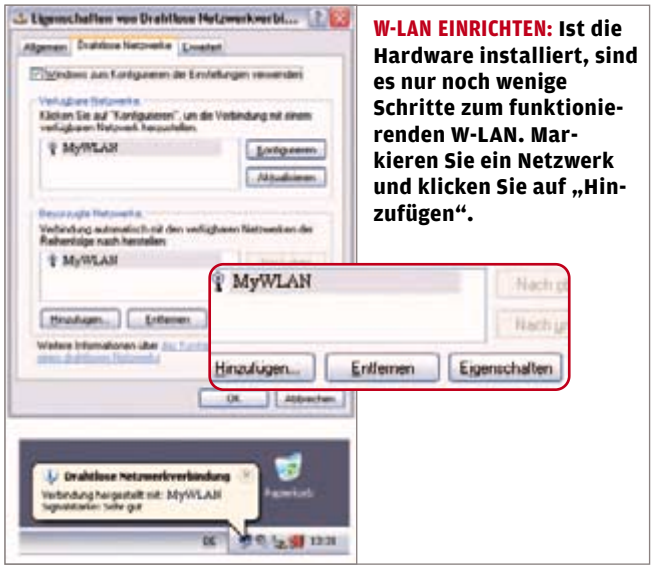
DIE VIER FUNKSTANDARDS FÜR EIN HEIMNETZWERK IM VERGLEICH

Standard	Datenrate (Netto)	Reichweite	Frequenz	Hotspot-Zugang	Leistungs-verlust	Interferenz	Kosten
802.11b	5 MBit/s	ca. 30 Meter	2,4 GHz	sehr gut	gering	hoch	niedrig
802.11g	20 MBit/s	ca. 50 Meter	2,4 GHz	sehr gut	gering	hoch	mittel
802.11a	22 MBit/s	ca. 30 Meter	5,0 GHz	schlecht	hoch	gering	hoch
Bluetooth	500 KBit/s	ca. 10 Meter	2,4 GHz	schlecht	gering	hoch	mittel

vorher überschwemmten die Hersteller den Markt mit neuer Hardware, noch bevor der Standard verabschiedet war. Die Folge war ein großes Firmware-Upgrade, sodass die Geräte schließlich auf dem letzten Stand der Spezifikationen waren. 802.11g hat zwei herausragende Merkmale, die ihn zum dominierenden Standard machen: der große Netto-Datendurchsatz von 22 MBit/s und die Rückwärts-Kompatibilität zu 802.11b. Die g-Version des Standards operiert auf dem gleichen Frequenzband wie die b-Version. Diese Vorteile machen 802.11g zur ersten Wahl, nicht nur beim Neuaufbau eines W-LANs, sondern auch als Erweiterung eines bestehenden drahtlosen Netzwerks. Der einzige Nachteil des Standards ist die Nutzung des Frequenzbereichs von 2,4 GHz, wo ein ziemliches Gedränge herrscht und die Konkurrenz aus Babyphones, Telefonen, Bluetooth und Mikrowellenherden den Empfang stören können.

Die Übertragungsraten in der Praxis

Vom Datendurchsatz können die drahtlosen Techniken mit einem Ethernet nicht mithalten, denn sobald sich eine Wand oder Mauer zwischen zwei Funkteilnehmern befindet, bricht die Geschwindigkeit ein. Deshalb weicht die tatsächlich erreichte Datenrate (Netto-Datenrate) in der Praxis fast immer von der nominellen Übertragungsrate ab. Durch Protokoll-Overhead, unvermeidliche Funklöcher, Reflexionen, Einstreuungen, Interferenzen und andere Störungen liegt die tatsächliche Datenrate durchschnittlich bei etwa 50 Prozent der theoretisch möglichen Brutto-Datenrate. Bei zunehmender Entfernung reißt die Verbindung bei Störungen nicht sofort ab, sondern wird durch Einsetzen der Fehlerkorrekturprogramme erst einmal langsamer. In mehreren Stufen (Fallback-Raten) schaltet die Verbindung auf die jeweils nächst niedrigeren Datentransferraten herunter. So werden Sie bei einem 802.11b-Netzwerk häufig nur mit etwa 5 bis 6 MBit/s rechnen können, was für eine Übertragung von originären Video-DVD-Daten in Echtzeit (etwa 10 MBit/s würden Sie dazu benötigen) bei weitem nicht ausreicht. Ältere W-LAN-Hardware nach 802.11b schafft nicht mal das Streamen von MPEG-2. Sie genügt lediglich den An-



W-LAN EINRICHTEN: Ist die Hardware installiert, sind es nur noch wenige Schritte zum funktionierenden W-LAN. Markieren Sie ein Netzwerk und klicken Sie auf „Hinzufügen“.

Die besten Multimedia-Tipps im Web

Alles zu Digital-Audio → www.cdburner.ca/digital-audio-formats-article Vergleich digitaler Audio-Formate
Suchmaschine → www.radio-locator.com
Links zu über 10.000 Internet-Radios und 2.500 Audio-Streams
Musik drahtlos → www.apple.com/airportexpress
Alles über Apples Musik-Server AirPort Express
Alle Codecs dieser Welt → www.codec-download.de
Codec-Download aus dem Archiv
Audio-Streaming → www.shoutcast.com/download/serve.phtml Die gesamte SHOUTcast-Server-Software zum Download

forderungen fürs drahtlose Übertragen von komprimierten Audio-Daten. Eine Möglichkeit, das Problem zu lösen, wäre, die DVD in das DivX-Format zu konvertieren, was den Bedarf an Transferrate auf etwa 4 MBit/s verringert. In den nächsten Zeilen finden Sie einige andere Übertragungsraten:

Audio-CD: 1,41 MBit/s
Dolby-Digital-Datenstrom: 0,5 MBit/s
DTS-Datenstrom: 1,5 MBit/s
MP3: 128 bis maximal 320 KBit/s
MPEG-2 (DVB-S-konform): 3 bis 4 MBit/s
MPEG-2 (SVCD-konform): 2,35 bis 2,8 MBit/s
Ogg Vorbis: maximal 300 KBit/s
WAV: 1.526 KBit/s

Hinzukommt: In einem W-LAN müssen sich alle Teilnehmer das gemeinsam benutzte Medium Funk, also die verfügbare Bandbreite auf den zulässigen Frequenzen, teilen. Nur einer darf zu einem bestimmten Zeitpunkt senden, damit die Übertragung klappt. Ein 54-MBit/s-W-LAN transportiert nur unter idealen Bedingungen einen MPEG-2-Datenstrom etwa von einer DVD oder als DVB-Aufzeichnung, sodass Sie ihn mit einem Streaming-Client störungsfrei genießen können. HDTV-MPEG-Daten oder ein zweiter Client überfordern 802.11g bereits. Schon das Übertragen eines vier GByte großen DVD-Image gerät im W-LAN zur Geduldsprobe: Selbst unter idealen Bedingungen dauert das immerhin rund eine halbe Stunde.

Drahtloses Home-Entertainment-Netz planen

Weil physikalische Hindernisse die drahtlosen Signale stören oder auslöschen können, ist die richtige Platzierung der Access Points im Haus überaus wichtig. Wenn Sie an dieser Stelle einen Fehler machen, können Sie eventuell nicht jeden Winkel des Hauses erreichen. Ermitteln Sie nach Möglichkeit die Größe des Bereichs, den Sie versorgen wollen und messen Sie die Signalstärke an den weit entfernten Punkten. Wi-Fi-Netzwerke funktionieren am besten in großen Räumen, während Sie zum Beispiel für Bluetooth mehrere Access Points benötigen, um die gewünschte Nähe herzustellen.

Ideal ist ein Lageplan, auf dem Sie erkennen können, wo der beste Standort für den Access Point ist. Der Sendebereich sollte nicht nur die Zimmer des Hauses (oder der Wohnung), sondern auch einen Außenbereich wie Balkon oder Terrasse abdecken. Dazu reicht oft schon ein einzelner Access Point. Drahtlose Netzwerke breiten sich horizontal und vertikal aus, je nach Konstruktion des Hauses können Sie damit auch das Stockwerk

über und unter dem Access Point abdecken. Bei massiven Hindernissen hilft auch die optimale Aufstellung des Access Points nicht weiter – dann benötigen Sie außerdem technische Lösungen wie Hochleistungsantennen, Ethernet-Kabel oder zusätzliche Access Points.

Jede Wand und jede Decke ist eine potenzielle Barriere für die elektromagnetischen Signale. Gipswände sind noch am leichtesten zu durchdringen, bei Stahlbeton wird es kritisch, da bleibt vom Signal oft nicht mehr viel übrig. Glas wirkt wie ein Reflektor, der das Signal zurückwirft. Wenn Sie kein Messgerät für die Signalstärke besitzen, müssen Sie in mehreren Versuchsdurchgängen den optimalen Aufstellungspunkt finden.

Welche Netzwerkgeräte Sie für Ihr W-LAN benötigen, ist am Anfang oft nicht ganz klar. Die Tabelle auf 88 wird Ihnen da weiterhelfen. Jedes Gerät, das Sie ans Netz anschließen wollen, braucht ein Sende- und Empfangsteil, um an der drahtlosen Kommunikation teilzunehmen.

In ältere Notebooks können Sie problemlos einen W-LAN-PC-Card-Adapter einbauen. Besonders komfortabel sind moderne Notebooks, bei ihnen gehört die W-LAN-Fähigkeit bereits zum Standard. Handheld-Computer verwenden zum Einstieg in die W-LAN-Welt meist CompactFlash-Erweiterungskarten – die sind allerdings recht teuer und haben eine sehr begrenzte Reichweite. Für Desktop-PCs gibt es USB- und PCI-Adapter. Wenn nicht alle Netz-Komponenten vom gleichen Hersteller stammen, sollten Sie auf das WiFi-Logo achten, um die Kompatibilität sicherzustellen.

In einem W-LAN kommunizieren alle Geräte über den Access Point. Ein Access Point agiert wie ein drahtloser Hub, sodass sich die angeschlossenen Computer die Netzwerk-Ressourcen wie Drucker, Laufwerke und/oder eine Breitbandverbindung teilen können. Aufgrund dieser Architektur können Sie sehr leicht weitere Geräte hinzufügen, ohne dass der Netzwerkbetrieb gestört wird. Erstreckt sich ein W-LAN über eine größere Fläche, ist oft die Aufstellung weiterer Access Points notwendig, um Funklöcher zu verkleinern oder auszuschalten. Auch die Verbindung mit einem Kabelnetzwerk geschieht über einen Access Point, der meistens auch als Router und Internet-Gateway fungiert.

Ein Router dient im internen Netzwerk als Schaltzentrale und stellt extern den sicheren Zugang zum Internet her. Über den Router können problemlos mehrere drahtlos verbundene Rechner gleichzeitig aufs Internet zugreifen. Unbedingt beachten sollten Sie, dass die Router-Software die neuesten Sicherheitsstandards (WEP und WPA) unterstützt. Ein Router mit einer eingebauten und gut konfigurierten Firewall schützt ein W-LAN vor unliebsamen Zugriffen aus dem Internet. Ganz wichtig ist, dass sich jede Netzwerkkomponente am Router anmelden muss.

Wenn Sie es versäumt haben, Ihr W-LAN abzusichern, kann jeder, der sich im Empfangsbereich Ihres Funknetzes aufhält, mit der entsprechenden Hardware in das W-LAN eindringen. Für die WEP-Verschlüsselung gibt es bereits zahlreiche Hacker-Tools, deshalb sollten Sie unbedingt die WPA-Verschlüsselung als Schutzmechanismus wählen. WPA ist außerdem abwärtskompatibel zu WEP; daher können durch Treiber- und Firmware-Updates bestehende Access Points und W-LAN-Karten auf WPA-Fähigkeit aufgerüstet werden.

Home-Entertainment-Netz einrichten

Nachdem alle Netzwerkkomponenten vorhanden sind, gilt es als nächstes, das W-LAN zum Laufen zu bringen.

1. Installieren Sie die Netzwerkkarten in allen Geräten, die an das W-LAN angeschlossen werden sollen. Auch wenn die Hardware nicht von unterschiedlichen Herstellern stammt, empfiehlt es sich immer, vorher die Installationshinweise in den Handbüchern zu lesen.

2. Soweit der Hardware-Hersteller nichts anderes vorschreibt, öffnen Sie unter Windows XP das Fenster „Netzwerkverbindungen“ und klicken mit der rechten Maustaste auf das Symbol „Drahtlose Netzwerkverbindung“.

3. Wählen Sie die Option „Eigenschaften“ aus dem Kontextmenü und aktivieren Sie anschließend die Registerkarte „Drahtlose Netzwerke“. →

KNOW-HOW

Die wichtigsten digitalen Audio-Formate

Name	Dateierweiterung	Ursprungsjahr	Qualität*	Hinweise
Advanced Audio Coding	.aac	1997	4	Auch bekannt als MPEG-4 AAC. Wird im iPod verwendet, unterstützt verschiedene Kompressionsraten
Audio Interchange File Format	.aiff	1999	3	Original Macintosh-Sound-Format, ohne Kompression
Compact Disk Digital Audio	.cda	1979	9	Original CD-Audio-Format, ohne Kompression
mp3PRO	.mp3	2001	2	Weiterentwickelte MP3-Version, wird kaum verwendet
MPEG-1 Level 3	.mp3	1993	9	Verschiedene Kompressionsraten, sehr häufige Verwendung
OGG Vorbis	.ogg	2000	4	OpenSource-Codec und Audio-Kompression
QuickTime Audio Video	.mov	1997	4	MPEG-4-Technik wie in AAC, wird selten verwendet
RealAudio Media	.rma	1995	3	Eigenständiges Audio-Format, geringe Verbreitung
Waveform Sound Files	.wav	1991	9	Windows System Sound
Windows Media Audio	.wma	1997	9	Verschiedene Kompressionsraten

* 1=schlecht; 10=gut

4. Im Feld „Verfügbare Netzwerke“ erscheint eine Liste der drahtlosen Access Points. Klicken Sie unter „Bevorzugte Netzwerke“ auf „Hinzufügen“.
5. Das Dialogfeld „Drahtlose Netzwerkeigenschaften“ erscheint. Geben Sie im Feld „Netzwerkname (SSID)“ den Namen des Access Points ein und aktivieren Sie die gewünschten Kontrollkästchen je nach den Erfordernissen Ihres Netzwerks. Für eine spätere Verwendung sollten Sie sich die Werte notieren.
6. Aktivieren Sie die Verschlüsselungs-Option und geben Sie den Schlüssel ein.
7. Lassen Sie die IP-Adresse automatisch von DHCP zuweisen.
8. Beenden Sie den Vorgang und schließen Sie alle Dialog-Fenster.

KNOW-HOW

So verbinden Sie Ihre Netzwerk-Geräte

Gerät	Verbindung
Router/Gateway	Breitband-Modem mit einem Access Point oder einer (W-LAN)-Netzwerkkarte
Access Point	Ethernet-Switch oder -Hub mit einer W-LAN-Netzwerkkarte
USB-Adapter	Computer mit einem Ethernet-Switch oder -Hub oder einen Access Point
PC-Netzwerkkarte	Computer mit einem Ethernet-Switch oder -Hub oder einen Access Point
Ethernet-Switch oder -Hub	Geräte mit einer Ethernet-Schnittstelle wie Media-Adapter, Router oder Switches
Wireless Media-Adapter/ Wireless Media-Server	Stereoanlage, Fernseher, AV-Receiver, Media Player, Computer

Sind alle Funknetzwerkkarten korrekt installiert, dauert es meistens nur ein paar Sekunden, bis Windows in der Taskleiste das Netzwerksymbol anzeigt. Dort erscheint ebenfalls ein Hinweisfenster darauf, dass ein neues Funknetz gefunden wurde. Wenn Sie mit der Maus über diesen Hinweis fahren, öffnet sich ein Dialogfenster, in dem die verfügbaren Funknetze angezeigt werden. Um Informationen über die Verbindung zu bekommen, klicken Sie zweimal auf das Symbol in der Taskleiste. Auf der Registerkarte „Details“ erhalten Sie Informationen über die IP-Adresse, den Router und die Subnetzmaske. Ihr W-LAN ist nun betriebsbereit und sollte sich auch nach einem Neustart wieder mit dem Router verbinden.

Verbindung herstellen mit einem Media-Adapter

Ein drahtloses Home-Entertainment-Netz ermöglicht die Wiedergabe digitaler Medien ohne lästiges Kabelverlegen. Um Ihren Computer mit der Unterhaltungselektronik zu verbinden, bieten die Hersteller einen Wireless Media-Adapter (Media-Streamer) an. Über den drahtlos verbundenen Media-Adapter können Sie etwa digitale Videos und Fotos auf dem Fernseher ansehen. Sie müssen sich auch nicht damit begnügen, Ihre digitale Musiksammlung auf den bescheidenen Computerlautsprechern anzuhören, sondern genießen sie in voller Klangstärke über die Stereoanlage. Ein Wireless Media-Adapter wird über Standardkabel an Stereoanlage und Fernseher angeschlossen. Der Kontakt zum Netzwerk erfolgt dann über eine drahtlose Verbindung oder ein normales 10/100-Ethernet-Kabel – falls Sie diese Variante bevorzugen. Während ein Kabelnetz vom Datendurchsatz her in den meisten Fällen ausreicht, ist bei der drahtlosen Variante ein Media-Adapter nach dem 802.11b-Standard für ein Video-Streaming zu schwach; dazu sollten Sie unbedingt ein 802.11g-Gerät einsetzen. Musikdaten bereiten bei einer maximalen Übertragungsrate von 320 KBit/s (MP3) auch dem langsameren 802.11b-Standard keine Probleme.

Im Lieferumfang eines Wireless Media-Adapters ist eine Fernbedienung enthalten, mit der Sie durch benutzerfreundliche Menüs auf Ihrem Fernseher oder durch die digitalen Bilder auf Ihrem PC blättern können. Angezeigt werden Ordner, Dateiname oder Miniaturansicht, die Bilder lassen sich auch zu einer automatisch ablaufenden Diashow zusammenstellen. Die meisten Media-Adapter unterstützen die gängigen Bildformate JPG, GIF, TIF und BMP. Mit der Zoom-Taste der Fernbedienung lassen sich die Bilder vergrößern und bestimmte Details anzeigen. Sie können auch mit der Fernbedienung Ihre MP3- oder WMA-Musikdateien nach Titel, Interpret, Stil, Ordner oder Playlist durchsuchen. Sie wählen Ihre Lieblingsmusik aus und der Wireless Media-Adapter spielt sie über die Stereoanlage ab. Während die Musik läuft, können Sie beispielsweise Ihre Bildersammlung durchsehen.

Wireless Media-Adapter arbeiten in der Regel nach dem 802.11g-Standard und sind per Funk mit einem Computer oder Access Point verbunden. Auf der Rückseite befinden sich meistens die folgenden Anschlüsse:
Audio-L/R-Ausgang (Stereo): Zum Verbinden des Geräts mit dem linken beziehungsweise rechten Eingang der Audio-Anlage
Ethernet-Konnektor RJ-45: Optionaler Ethernet-Anschluss für ein kabelgebundenes Heimnetz. Dafür sollten Sie ein abgeschirmtes CAT5-Ethernet-Kabel (STP) verwenden.
SCART (EURO): Audio-/Video-Ausgang zum Fernsehgerät

Rein technisch gesehen lässt sich mit einem solchen Gerät als drahtloser TV-Link jedes beliebige Videosignal (digitale oder analoge Set-Top-Boxen, DVD-Spieler, Satellitenempfänger, Videorecorder etc.) oder Kabelprogramm (über den Videorecorder) im gesamten Haus weiterleiten.

Die Konfiguration eines Wireless Media-Adapters nehmen Sie mit dem Web-Browser am PC vor. In vielen Fällen sind Sie gut beraten, sich zunächst die neueste Treiber-Version von der Hersteller-Homepage herunterzuladen. Vorsicht: Zur Konfiguration ist es erforderlich, sämtliche Firewall- und Sicherheitssoftware zu deaktivieren. Rufen Sie anschließend die Management-Oberfläche für den Adapter auf. In den meisten Fällen werden Sie von einem Assistenten durch die mitunter recht umfangreiche Konfiguration geführt.

Media-Adapter sind werkseitig in der Regel so vorkonfiguriert, dass sie automatisch mit Ihrem PC und dem Internet Verbindung aufnehmen und zwar entweder über eine Punkt-zu-Punkt-Verbindung oder über ein Heimnetzwerk mit einem Breitband-Internetzugang.

KNOW-HOW

Bitraten der Audio- und Video-Formate

Medium	Format	Auflösung/Sample-Frequenz	Maximale Bitrate
Film	MPEG-1	720 x 576	1,5 MBit/s
Film	MPEG-2	720 x 576	8 MBit/s
Film	DivX Version 4	720 x 576	6 MBit/s
Film	DivX Version 5	720 x 576	8 MBit/s
Film	XviD	720 x 576	8 MBit/s
Audio	WMA Version 8 u. 9	32/44,1/48 kHz	192 KBit/s
Audio	WAV	44,1/48 kHz	
Audio	MP3	32/44,1/48 kHz	32 bis 320 KBit/s
Audio	Ogg Vorbis	variabel	64 bis 256 KBit/s
Audio	WMA	64 kHz	160 KBit/s

Punkt-zu-Punkt-Verbindung: Über den Wireless USB-Adapter wird der Media-Adapter mit dem PC verbunden, um die Streams drahtlos auf dem Fernseher oder der HiFi-Anlage, die sich in verschiedenen Räumen oder Stockwerken befinden können, wiederzugeben. Die Steuerung erfolgt über das Menü des Media-Adapters.

Heimnetzwerk mit Breitband-Internet: Um auf einfache Weise nicht nur auf Ihre eigenen Dateien, sondern auch auf die gesamten im Internet verfügbaren Musiktitel, Filme, Fotos oder Spiele zugreifen zu können, schließen Sie den Media-Adapter an Ihren Breitband-Internetzugang an. Danach können Sie auf einem oder mehreren PCs oder anderen WiFi-Geräten überall im Haus ein grenzenloses Unterhaltungsangebot genießen.

AV-Receiver/DVD-Player ins W-LAN einbinden

Nachdem alle Desktops, PDAs und Notebooks ins W-LAN integriert wurden und das drahtlose Netzwerk funktioniert, ist es an der Zeit, einen netzwerkfähigen AV-Receiver oder einen DVD-Player in das W-LAN einzubauen. Auf den ersten Blick ist das nicht ganz einfach, denn die auf dem Markt befindlichen Geräte besitzen noch keinen W-LAN-Adapter.

Eine Lösung des Problems wäre die Anbindung an einen Access Point, der als Bridge zum drahtlosen Netzwerk dient. Haben Sie gleichzeitig ein Access Point im Einsatz, der als W-LAN-Router fungiert, müssen Sie die Geräte so konfigurieren, dass sie sich gegenseitig „verstehen". Das ist nicht immer ganz einfach, wenn die Geräte von verschiedenen Herstellern stammen. Da kann es schon mal vorkommen, dass Access Point und Router nicht miteinander kommunizieren wollen. In diesem Fall hilft nur Testen und Ausprobieren. Schon aus diesem Grund empfiehlt es sich, nur die Geräte eines Herstellers verwenden. Ein Access Point, der nach dem IEEE-802.11g-Standard 54 MBit/s verkraftet, ist in normalen Raumumgebungen mehr als ausreichend dimensioniert für Video-Streaming.

Video-Streaming mit VideoLAN

Um Ihr drahtloses Home-Entertainment-Netz fit für Video-Streams zu machen, können Sie auf die OpenSource-Software VideoLAN (auf Heft-DVD) von der „École Centrale Paris" zurückgreifen. Das Programm ist für alle gängigen Betriebssysteme erhältlich. Bei der Streaming-Software wird zwischen dem VideoLAN-Server (VLS) und dem VideoLAN-Client (VLC) unterschieden. Das Programm ist multilingual, also auch mit deutscher Benutzeroberfläche erhältlich. Zum Streaming von Videos benötigen Sie allerdings nicht unbedingt die Server-Version, auch VLC kann folgende Dateien lesen:

MPEG-1-, MPEG-2- und MPEG-4-/DivX-Dateien von einer Festplatte oder einem CD-ROM-Laufwerk

DVDs und VCDs

Daten von einer Satellitenkarte (DVB-S) →

KNOW-HOW

Die wichtigsten digitalen Video-Formate

Format	Dateiendung	Bemerkung
Audio Video Interleaved (AVI)	.avi	Von Microsoft definierter Container für Multimedia-Formate, das von dem für Windows 3.1 eingeführten RIFF (Resource Interchange File Format) abgeleitet ist. AVI ist auf Microsoft-Windows-basierenden Systemen der De-facto-Standard für Audio- und Videodaten.
QuickTime Audio Video	.mov	Von Apple-Computern genutztes Audio- und Videoformat
MPEG-4	.mp4 u.a.	Von der „Motion Picture Experts Group" entwickeltes Dateiformat, das auf dem Apple-QuickTime-Dateiformat basiert und in ISO/IEC 14496-12 und -14 (MPEG-4 Part 12 und 14) standardisiert wurde. In MP4-Dateien können multimediale Inhalte in Form von mehreren Audio- und Videospuren sowie Untertitel, 2D- und 3D-Grafiken und Bilder gespeichert werden. Diese Inhalte lassen sich dann mit Hilfe geeigneter Software übers Internet streamen.
MPEG	.mpg u. a.	Fortschrittliches Videoformat, das als MPEG-1 oder MPEG-2 unter anderem für Video-CDs, DVD-Videos und DVB sowie Tonformate in Fernsehqualität verwendet wird.
Ogg Media (OGM)	.ogm	Mehrere Tonspuren in verschiedenen Sprachen sowie Untertitelspuren und Kapitelgliederungen sind möglich (wie auf einer DVD). Dieses Format wurde hauptsächlich entwickelt, um den Ogg-Vorbis-Audiocodec in einem Video wiederzugeben. Dies ist mit AVI nicht möglich.

MPEG-1-, MPEG-2- und MPEG-4-Streams aus dem Netzwerk, gesendet von VLS oder VLCs

Auf die mitunter recht komplexe Server-Konfiguration können Sie verzichten und VideoLAN-Client als Streaming-Server verwenden, wenn Sie MPEG-1-, MPEG-2-, MPEG-4-/DivX-Dateien und DVDs von einer MPEG-Kodierungskarte an eine IP-Adresse (Unicast) oder an eine Gruppe von IP-Adressen (Multicast) senden wollen.

Mit VLC ist es möglich, Übertragungskanäle zu mehreren Clients festzulegen und Nutzerprofile mit bestimmten Zugriffsrechten anzulegen. Hardwareseitig gibt sich VLC mit einem 1,5-GHz-Pentium-Prozessor mit 512 MByte Hauptspeicher zufrieden. Auf der Festplatte sollten mindestens 40 GByte Platz sein. VLC verfügt je nach Betriebssystem über verschiedene grafische Oberflächen und Skins, kann aber auch von der Befehlszeile oder per Makro gesteuert werden. Zur Installation unter Windows genügt ein Doppelklick auf die selbstextrahierende Datei. Bevor Sie VLC einsetzen, sollten Sie allerdings ein paar Einstellungen vornehmen:

1. Wählen Sie im Datei-Menü die Option „Streaming-Assistent“ (Kombination [Strg]+[W]) und klicken Sie auf „Über das Netzwerk streamen“. Klicken Sie danach auf „Next“.

2. Im nächsten Fenster klicken Sie auf „Wählen“ und öffnen die Registerkarte „DirectShow“. Klicken Sie anschließend unter „Video-Devicename“ auf „Refresh List“. Wählen Sie anschließend aus der Liste Ihre TV-Karte aus. Wiederholen Sie diesen Schritt für „Audio-Devicename“ und wählen Sie an dieser Stelle die Soundkarte aus.

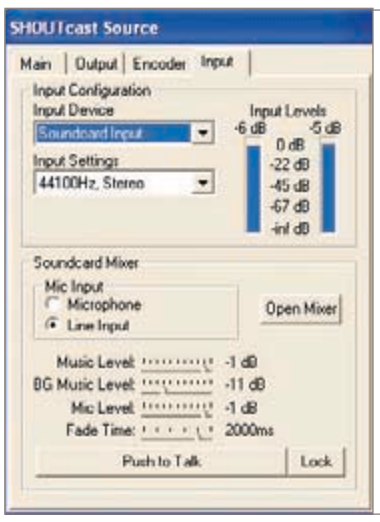
3. Setzen Sie zum Schluss das Häkchen bei „Device-Eigenschaften“.

4. Aktivieren Sie die Registerkarte „Netzwerk“. Geben Sie in die Adresszeile die Adresse des Streams ein, den Sie wiedergeben möchten. Klicken Sie dann auf „Next“.

5. Wählen Sie die Streaming-Methode (Unicast oder Multicast) und geben Sie die Adresse des Zielcomputers (eigener Rechner = localhost) ein. Klicken Sie dann erneut auf „Next“.

6. Wählen Sie als Verkapselungsmethode „MPEG TS“ und klicken Sie wieder auf „Next“.

7. Tragen Sie unter „Time To Live“ den Wert „12“ ein. Das sollte auch für die Übertragung in langsamen Netzwerken reichen.



MUSIK ÜBERALL: Mit dem SHOUTcast Server werden Audio-Streams an einen oder mehrere Clients ins drahtlose Home-Entertainment-Netz ausgestrahlt.

Klicken Sie anschließend auf „Finish“ und kehren Sie ins Hauptfenster zurück.

MPEG-2-Multicast erfordert eine Bandbreite von mindestens 3,5 MBit/s, um vernünftig zu funktionieren. Benutzerhandbücher und Support finden Sie auf der VideoLAN-Homepage (**www.videolan.org** oder **forum.videolan.org**).

Audio-Streaming mit Shoutcast

Sind die digitalen Audio-Dateien erst einmal auf einem PC gelandet, müssen Sie diese in ein „Streaming-Audioformat“ umwandeln, wenn Sie sie über das LAN oder W-LAN senden wollen. Nur so kann ein Streaming-Server sie via TCP/IP paketweise an die angeschlossenen Clients senden. Streaming-Audio-Daten gibt es in vielen Formaten:

MP3 (SHOUTcast)
AAC (Advanced Audio Coding, wird von iTunes verwendet)
WMA (Windows Media Audio)
Andere (etwa Real Media Audio)

Jeder Audio-Stream hat seine eigene Bitrate. Die Bitrate definiert die Anzahl an Paketen, die pro Sekunde gesendet werden. Höhere Bitraten sind natürlich besser als niedrige, erfordern aber eine schnelle Internet-Anbindung.

Internet-Radios bieten einen guten Einstieg in die Welt des Audio-Streaming. Heute gibt es unzählig viele Radiostationen, die ihr Programm über das Internet verbreiten. Die komfortabelste Art, diese Streams zu empfangen, ist ein Media-Player wie Winamp 5 oder der Windows Media Player 10. Auch für das Streaming via W-LAN gibt es viele Lösungen. Eine der einfachsten Möglichkeiten, Musik über ein drahtloses Netzwerk zu senden, ist die Installation eines SHOUTcast-Servers. Dazu benötigen Sie:

Winamp Version 5
SHOUTcast Server-Software
DSP-Plugin

Sie bekommen die gesamte benötigte Software kostenlos unter **www.shoutcast.com**. Laden Sie dort die neuesten Versionen herunter. Installieren Sie zuerst Winamp, danach das DSP-Plugin und zum Schluss die SHOUTcast-Software. Der Server streamt das Audio-Signal, das er von Winamp und vom DSP-Plug-In bekommt, zu den angeschlossenen Clients. Außerdem ist es möglich, MP3-Dateien, die auf der Festplatte gespeichert sind, auf Anforderung zu übertragen.

1. Nach der Installation der drei Software-Pakete wird zunächst das DSP-Plugin aktiviert. Wählen Sie dazu die Option „Preferences“ aus dem Menü „Options“.

2. Klicken Sie nun im Fenster „Preferences“ auf „DSP/Effect“. Wenn Sie alles richtig gemacht haben, sehen Sie jetzt im rechten Fenster „Nullsoft SHOUTcast Source DSP v.1.9.5b [dsp_sc.dll]“.

3. Schließen Sie anschließend das Fenster „Preferences“.

4. Klicken Sie zweimal auf das Symbol „Edit SHOUTcast DNAS configuration“ aus der Programmgruppe „Shoutcast DNAS“, die das Installationsprogramm angelegt hat. Ändern Sie als erstes das Default-Passwort. Die übrigen Optionen brauchen Sie nicht zu ändern, sofern nicht mehr als 32 Clients „zuhören“.

5. Öffnen Sie nun die „Network Configuration“. Unter „SrcIP“ finden Sie die Adresse, von der der Server Broadcast empfängt.

An dieser Stelle sollte die IP-Adresse „127.0.0.1“ erscheinen.
6. Unter „DestIP“ tragen Sie die Adressen der Clients ein, an die der Stream gesendet werden soll.
7. Weiter unten finden Sie die „Server Configuration“. Dort setzen Sie die Option „Public Server“ auf „PublicServer=never“. Die Werte für „AllowRelay“ und „AllowPublicRelay“ müssen beide auf „No“ gesetzt sein.

Damit ist die Konfiguration des SCOUTcast-Servers abgeschlossen. Um einen Stream zu hören, wählen Sie die Option „Play URL“ aus dem Player-Menü. Geben Sie dann die IP-Adresse des Servers in Ihrem Heimnetzwerk ein, gefolgt von einem Doppelpunkt und „8000“. Geben Sie also beispielsweise „192.168.0.2:8000“ ein, wenn die Adresse des IP-Servers 192.168.0.2 lautet. Peter Klau

KNOW-HOW

Filme, Musik und Bilder aus dem Internet

Film ab im Internet Ein Home-Entertainment-Netz ermöglicht Ihnen den direkten Zugriff auf Film-Trailer, Musik-Videos und Kurzfilme aus dem Internet.

Name	Adresse	Infos
Yahoo Movies	movies.yahoo.com	Eine der besten Entertainment-Sites im Web. Yahoo Movies bietet die weltweit beste Auswahl an Kino-Trailern.
LAUNCH music videos	lauch.yahoo.com	Die größte Auswahl an Musik-Videos im Web
iFilm	www.ifilm.com	Bei iFilm finden Sie eine Riesenauswahl an Kurzfilmen und Video-Clips – die Super-Site für Filmfans und Filmemacher.

Netzmusik – die Internet-Radios Hören Sie sich Musik und Beiträge an, die es nur bei den Internet-Radios gibt: CD-Tipps, Lyrix und Infos über neue Trends. Die Channels werden rund um die Uhr als Schleife gespielt. Einige deutschsprachige Radiosender bieten ihr Programm als variablen Stream an. So ist gewährleistet, dass auch Hörer, die keinen DSL-Anschluss besitzen, in den Genuss hochqualitativer Übertragungen kommen.

Name	Adresse	Infos
Andante	www.andante.com	Lieben Sie klassische Musik? Dann ist Andante für Sie die richtige Website, außerdem ein neues Plattenlabel, das sich der Bewahrung klassischer Musik als Kulturerbe widmet. Andante ist ein echter On-Demand-Audiodienst und ermöglicht Ihnen eine Suche nach Musikrichtung, Interpret und Titel.
Gracenote	www.gracenote.com	Bei Gracenote können Sie automatisch und in Sekundenschnelle Informationen über Album, Interpret und Titel abrufen und Ihre digitalen Musiktitel verwalten.
LAUNCHcast	launch.yahoo.com	Ein werbefreier Musiksender im mp3PRO-Format für qualitativ hochwertigen Sound auf Ihrem Home-Entertainment-Netz.
Live365	www.live365.com	Live365 ist das weltweit größte Internet-Radionetzwerk mit Tausenden von Sendern aus über 200 Ländern. Die Premium-Dienste von Live365 liefern werbefreie Musik und Hunderte von VIP-Sendern.
MusicMatch	www.musicmatch.com	MusicMatch bietet eine umfassende Auswahl von Musikdiensten, darunter eine Vielfalt von Musiksendern, die nach Interpreten und Musikrichtung klassifiziert sind. Hier können Sie Ihre Lieblingssender zusammenstellen, die nach Interpret, Musikrichtung und Sendezeit auszuwählen sind.
My Streams	www.shoutcast.com	Mit My Streams können Sie praktisch jeden MP3-/mp3PRO-Musiktitel aus dem Internet auf Ihrem Home-Entertainment-Netz anhören und der Auswahlliste eigene Sender hinzufügen.
PlayhouseRadio	www.playhouseradio.com	Ein Musiksender speziell für Kinder mit einem großen Songarchiv englischer Kinderlieder.
Radio Free Virgin	www.radiofreevirgin.com	Qualitativ hochwertiges Musikprogramm, das nach Musikrichtung, Lifestyle und Herkunft klassifiziert ist.

Bilder saugen Online-Fotos – umfassende Sammlungen professioneller Fotos von den interessantesten Orten auf unserem Globus.

Name	Adresse	Infos
Yahoo Photos	photos.yahoo.com	Fotos gegen Gebühr downloaden und speichern oder eine eigene Diashow zusammenstellen
Born To Shoot	www.borntoshoot.com	Preisgekrönte Fotosammlungen im eigenen Netzwerk verwenden und als Diashow präsentieren
Google Bilder	images.google.de oder images.google.com	Bilder aller Art nach Schlüsselwörtern suchen. Vorsicht, Copyright beachten!

Sicherheit per W-LAN

Optische Raumüberwachung

Sicherheit ist in den letzten Jahren ein großes Thema geworden, wobei sehr unterschiedliche Beweggründe eine Rolle spielen. In modernen Sicherheitskonzepten wird die Videoüberwachung immer wichtiger. In diesem Beitrag erfahren Sie, wie Sie eine Überwachungsanlage aufbauen und in Betrieb halten.

Videoüberwachungstechnik galt bisher als extrem aufwendig und kostspielig. Fand man bisweilen Kameras auf einem Grundstück, handelte es sich entweder um eine Video-Anlage für die Torsprechanlage aus dem Baumarkt, einen „Dummy“ ohne Funktion oder um ein echtes System mit abschreckender Wirkung. Videoüberwachung hat aber noch einen weiteren Vorteil, wenn ein solches System ergänzend zu einer Alarmanlage eingesetzt wird. In dieser Konstellation trägt ein gutes Videoüberwachungssystem zur Bestätigung eines Alarms und damit zur Vermeidung von teuren Fehleinsätzen der Polizei oder eines Sicherheitsdienstes bei.

Videoüberwachungstechnik kann aber auch einem Pflegedienst sehr nützlich sein. Ältere, gebrechliche Menschen können oft nicht in ihrer vertrauten Wohnung bleiben, weil im Notfall nicht schnell genug medizinische Hilfe angefordert werden kann. Durch Videoüberwachung sind Angehörige in der Lage, auch ohne lokale Präsenz regelmäßig nach dem Rechten zu sehen und bei Bedarf umgehend medizinische Hilfe anzufordern. Zwar berührt ein solches System die persönlichen Rechte der „überwachten“ Person. Auf der anderen Seite lässt sich damit die Unterbringung in einem Altenheim vermeiden.

Optische Überwachungsszenarien

Eine optische Überwachung kann in unterschiedlichsten Formen stattfinden: Eine Möglichkeit ist beispielsweise die permanente Überwachung durch eine oder mehrere Kameras auf einem Monitor beziehungsweise die permanente Aufzeichnung der Bilder. Dieses Verfahren garantiert zwar eine lückenlose Überwachung des beobachteten Bereiches, allerdings werden dabei überwiegend irrelevante Ereignisse erfasst, was den Beobachter schnell ermüden und möglicherweise die eigentlich wichtigen Dinge übersehen lässt.

Effektiver ist es dagegen, wenn die Kamera ereignisgesteuert aktiviert wird. Das hat verschiedene Vorteile, denn einerseits trifft das Ereignis auf die volle Aufmerksamkeit des Beobachters und zudem spart es erhebliche Ressourcen ein – beispielsweise Band- oder Festplattenkapazitäten und gegebenenfalls Übertragungsbandbreite.

Eine dritte Variante ist die bedarfsweise Aktivierung der Videokamera durch den Beobachter selbst. Das setzt voraus, dass dieser die Kamera gezielt über einen Verbindungsweg ansteuern und aktivieren kann. Dieses Prinzip ist für Routine-Überwachungen gut geeignet, allerdings für eine Alarmanlage nur begrenzt von Nutzen.

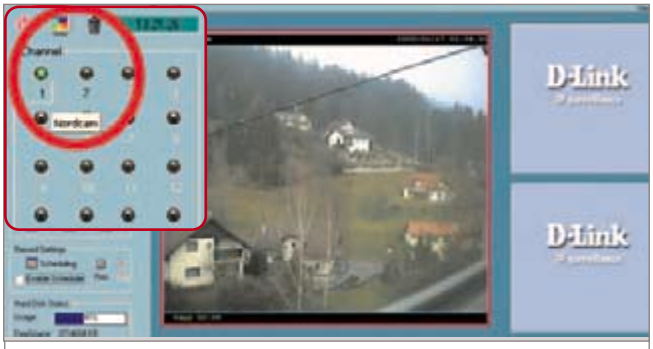
Ideal ist die Kombination aus einer ereignisgesteuerten Aktivität und der bedarfsweisen Zugriffsmöglichkeit auf die Kameras, die dem Beobachter die optimale Flexibilität bei seiner Überwachungsaufgabe bietet.

Alarmzentrale mit bis zu 16 Kameras einrichten

In einem ersten Beispiel sollen die Einsatzmöglichkeiten einer modernen Videoüberwachungsanlage am Beispiel der IP-Surveillance-Software des Kamera-Modells DCS-5300W von D-Link vorgestellt werden. Damit lassen sich bis zu 16 Kameras auf einer Oberfläche verwalten.

Um eine Kamera in diese Oberfläche zu integrieren, muss sie zunächst in das Netzwerk eingebaut werden. D-Link liefert dazu den IP Installer mit, mit dessen Hilfe die Netzwerkadressen und eventuelle Verschlüsselungen der Kamera-Datenströme aktiviert werden. Anhand der IP-Adresse erfolgt die Anmeldung der Kamera in der Überwachungssoftware und die Zuweisung zu einem Überwachungskanal. In der detaillierten Konfiguration jeder einzelnen Kamera empfiehlt es sich, ihr zunächst einen Namen zu geben, der im jeweiligen Fenster erscheint. Der Name sollte so aussagekräftig sein, dass in komplexen Systemen einem Wachmann die sofortige Zuordnung der Kamera mit dem entsprechenden Einsatzort möglich ist.

Damit das Bild einer Kamera angezeigt werden kann, muss der entsprechende Channel mit der Maus in das gewünschte Fenster des Layouts gezogen werden. Insgesamt sind sechs Layouts vordefiniert. Das Channel-Fenster gibt anhand der Icons Aufschluss darüber, welche Kanäle im Layout platziert oder zumindest verfügbar sind. Anhand der Farbe des Icons kann der Benutzer darüber hinaus sofort erkennen, ob gerade eine Videosequenz aufgezeichnet wird oder ob sich die Kamera im reinen Beobachtungsmodus befindet.



ALLES IM BLICK: Zwei der insgesamt 16 Channels sind mit jeweils einer Kamera belegt, was die dunklen Zahlen signalisieren. Lediglich Channel 1, die „Nordcam“, ist bereits im Layout installiert. Dies zeigt das grüne Kontrollfeld an.

Die von den Kameras erfassten Bilder können gezielt – beispielsweise auf die Festplatte des Monitor-PCs – aufgezeichnet werden. Dazu stehen drei Optionen zur Wahl: Auf der einen Seite kann die Aufnahme von einem Ereignis gesteuert werden (Motion Detection). Die Aufzeichnung startet, sobald sich das Kamerabild verändert und endet nach Ablauf einer vorgegebenen Zeitspanne. Damit nicht gleich jeder vorbeifliegende Vogel eine Aufnahme auslöst, lässt sich die Empfindlichkeit und die prozentuale Größe des für einen Alarm zu verändernden Bildinhaltes individuell vorgeben.

Die zweite Option sieht eine zeitgesteuerte Aufzeichnung vor. Dazu dient ein Scheduler, der entweder zu einem exakt definierten Termin oder in regelmäßigen Intervallen die Aufzeichnung der Bilder der ausgewählten Kamera startet und beendet. Neben den beiden automatisierten Aufzeichnungsoptionen steht dem Beobachter auch die Möglichkeit einer spontanen Aufzeichnung offen. Dazu klickt er zuerst in das Layout auf die gewünschte Kamera und aktiviert anschließend im Steuerbereich der Software die Aufnahme.

Kamera als Bewegungsmelder

Speziell der Bereich Motion Detection ist für ein Überwachungssystem interessant, denn diese Funktion ersetzt einen herkömmlichen, passiven Bewegungsmelder. Mehr noch: Durch die Möglichkeit, konkrete Bildausschnitte für die Überwachung von Bewegungen und zudem Empfindlichkeitsstufen definieren zu können, arbeitet diese Funktion weitaus präziser als ein passiver Bewegungsmelder. Welche Einstellungen für die Empfindlichkeit und die prozentuale Bildänderung zu wählen sind, die letztlich den Alarm auslösen, muss nach den Gegebenheiten der Umgebung sowie den vorherrschenden Lichtverhältnissen individuell ermittelt werden. An dieser Stelle ist – das zeigte der Test der Kamera für diesen Beitrag – besonders große Sorgfalt erforderlich.

Das Objektiv der schwenkbaren Kamera erfasst natürlich immer nur einen Teil der Umgebung. Aus diesem Grund gibt es für den Beobachter verschiedene Möglichkeiten, die Kamera fernzusteuern. Das hat den Vorteil, dass zur Überwachung größerer Bereiche nur vergleichsweise wenige Kameras notwendig sind. Insgesamt stehen dem Beobachter vier Steuerungsmöglichkeiten für jede Kamera zur Verfügung.

Wünscht der Beobachter, spontan einen ganz bestimmten Bereich zu betrachten, kann er das Kamera-Objektiv mit Hilfe von horizontalen und vertikalen Pfeilschaltflächen manuell ansteuern und bewegen. Oft bietet es sich an, die Navigation des Objektivs aus der Grundposition heraus zu beginnen. Dazu steht eine eigene Schaltfläche zur Verfügung. Wird sie aktiviert, bewegt sich das Objektiv – egal wie es zuvor ausgerichtet war – in die neutrale Startposition zurück.

Der Beobachter muss Kompromisse zwischen der Zielsteuerung und der Geschwindigkeit machen. Wünscht er hohe Präzision, wählt er in den Grundeinstellungen der Kamera eine kurze Schrittweite. Soll die Kamera aber möglichst schnell schwenken, muss die Schrittweite entsprechend vergrößert werden. Zugriff auf die Grundeinstellungen der einzelnen Kameras erhält der Beobachter beziehungsweise der Systemadministrator über das Menü „Function“.

PROFI-TIPP

Unterwegs zuhause reinschauen

Viele Urlauber fragen sich immer wieder, ob denn zuhause auch alles in Ordnung ist. Ist der Herd wirklich ausgeschaltet, oder wurde möglicherweise eingebrochen? Eine Videokamera mit Netzwerkanschluss – idealerweise W-LAN, um sie ohne viel Aufwand installieren zu können – und einen DSL-Anschluss benötigt man, um von unterwegs aus mal eben nach Hause schalten zu können. Die Kamera ist dabei ein Webserver, der über den DSL-Anschluss direkt am Internet angebunden ist. Ein Passwortschutz für den Zugriff auf die Kamera verhindert, dass die falschen Augen die Wohnung sondieren.

Dynamische IP-Adresse **Ein Problem teilen alle privaten Internet-Zugänge: die dynamische IP-Adresse. Auch dafür gibt es mittlerweile eine Lösung für jedermann: Dynamic DNS, DynDNS oder DDNS. Unterstützt die Kamera den dynamischen Domain Name Service, muss der Betreiber lediglich eine Domain bei einem entsprechenden Anbieter (unter www.dyndns.org auch kostenlos möglich) anmelden. Diese Adresse wird in die Konfiguration der Kamera eingetragen, die sich mit ihrer jeweils aktuellen IP-Adresse beim Dienstleister anmeldet. Die Aktualisierung der IP-Adresse erfolgt in regelmäßigen Abständen oder bei Veränderungen der Adresse, sodass die Kamera selbst nach einer Zwangstrennung allenfalls nur für kurze Zeit nicht erreichbar ist.**

Kamera-Zugriff **Über einen Computer in einem Internet-Café, über das Notebook in einem W-LAN-Hotspot oder über einen Mobilfunk-Zugang erfolgt der Zugriff auf die Kamera. Im letzten Fall wird allerdings die Bandbreite bei GSM-Mobilfunkdiensten für hochauflösende Videosequenzen mit rascher Bildwechselfrequenz nicht ausreichend sein. Im Browser trägt man dann als Adresse die DynDNS-Adresse – etwa „meinname.dyndns.biz“ – ein. Nach der Authentifizierung durch Benutzername und Passwort kann anschließend der Zugriff auf die Videokamera erfolgen.**

EIGENE DOMAIN: DynDNS.org bietet Systemen, die mit dynamischen IP-Adressen im Internet arbeiten, kostenlos eine DynDNS-Adresse.

Eine gute Kombination aus Präzision und Geschwindigkeit bietet die gezielte Auswahl namentlich benannter Positionen. Auch an dieser Stelle ist die Grunddefinition in den Kameras die Voraussetzung, um eine Position mit dem Dropdown-Menü wählen zu können. Sind wichtige Positionen vordefiniert, erleichtert dies dem Beobachter die Arbeit erheblich. Eine Erweiterung dieser Funktion ist das automatische Anfahren der namentlich definierten Positionen in einer vorgegebenen Reihenfolge (Patrol). Das Objektiv bleibt dann eine gewisse Zeit in dieser Position stehen, wobei diese Verweildauer vom Administrator in Sekunden vorgegeben werden kann. Erst nach Ablauf der Verweildauer richtet die Kamera das Objektiv automatisch auf die nächste Position aus. →

Bei der vierten Möglichkeit handelt es sich ebenfalls um einen automatischen Schwenk des Objektivs; allerdings wird dieser Schwenk ausschließlich in horizontaler Richtung durchgeführt, wobei die Kamera einen kompletten Zyklus vom aktuellen Startpunkt über die beiden horizontalen Grenzpunkte zurück zum Startpunkt beschreibt. Eine Vordefinition von Positionen ist dabei nicht notwendig.

Videoüberwachung mit Sprachdialog

Das Kamera-System Mobotix M10D, das wir für diesen Beitrag getestet haben, besteht aus einer Dualoptik für den Tag- und den Nachtbetrieb, wobei die Kamera das Umschalten auf das jeweils optimale Objektiv automatisch übernimmt. Die Mobotix-Kameras verfügen zwar nicht von Haus aus über eine W-LAN-Schnittstelle. Sie sind jedoch mit einer RS232-, einer ISDN-S0- und einer Ethernet-Schnittstelle ausgerüstet, und mit Hilfe eines einfachen Medienkonverters lässt sich die Kamera problemlos in ein drahtloses Netzwerk integrieren. Dabei kann es sich beispielsweise um einen relativ preiswerten W-LAN-Access-Point handeln, der entsprechend konfigurierbar ist.

Durch die mögliche Kombination von ISDN-Wählanschluss und IP-Netzwerk ist es machbar, die Kamera gezielt über das Wählnetz anzusteuern und die eigentlichen Überwachungsaufnahmen kostengünstig via IP-Netzwerk zu übermitteln. Darüber hinaus lässt sich über den integrierten Lautsprecher und das Mikrofon in der Kamera ein direkter Dialog zu den Personen vor Ort herstellen.

PROFI-TIPP

Fehlalarme minimieren

Viele Alarme, die in den Wachzentralen auflaufen, entpuppen sich als Fehlalarme. Sie werden ausgelöst durch Fehler in den Systemen, durch Tiere auf dem überwachten Gelände oder andere Störeinflüsse. Rückt infolge eines solchen Fehlalarms ein Wachschutzmitarbeiter oder sogar die Polizei aus, wird es für den Betreiber der Alarmanlage sehr teuer. Abgesehen davon verliert eine Alarmanlage bei zu vielen Fehlalarmen ihre Wirkung, und selbst Nachbarn reagieren aus Unsicherheit nicht mehr auf ein Signal.

Die Kamera klärt auf **Mit einem ergänzenden Videoüberwachungssystem lässt sich nun ziemlich zuverlässig prüfen, ob der übermittelte Alarm echt ist oder durch eine Störung ausgelöst wurde. Auf die Dauer amortisiert sich in diesen Fällen aufgrund der unterbundenen Fehlalarme das Videosystem selbst dann, wenn möglicherweise niemals der Ernstfall eines Einbruchs eintritt.**

Um die Kamera über das ISDN anzurufen, muss ihr zunächst eine Rufnummer in der Konfiguration zugewiesen werden. An dieser Stelle lassen sich zwei wichtige Sicherheitsbarrieren definieren.

Auf der einen Seite sieht die Kamera die Abfrage einer PIN nach Annahme des Rufs vor. Zusätzlich wertet die Kamera bei Bedarf die Rufnummer des Anrufers aus. Soll die Kamera auf ein Ereignis reagieren und einen Alarm per ISDN-Anruf an ei-

PRODUKT-TIPPS

Kamera D-Link DCS-5300W

Die DCS-5300W ist eine motorgesteuerte Kamera, die mit einer Ethernet- und einer W-LAN-Schnittstelle ausgestattet ist. Die Unterstützung des H.263+/MPEG4 Short-Header-Modus sorgt für hochwertige Bilder, deren Qualität und Bildwechselfolgen an die Eigenschaften des Netzwerks angepasst werden können. Ein integriertes Mikrofon ermöglicht die gezielte akustische Überwachung.

Ausrichtung und Zoom der Kamera lässt sich per Software am PC fernsteuern. Darüber hinaus lassen sich Kamerapositionen definieren, die in einer beliebigen Reihenfolge automatisch angefahren werden (Patrol). Außerdem ist ein horizontaler automatischer Schwenk möglich (Pan).

Die Videosequenzen lassen sich manuell oder ereignisgesteuert für die Beweissicherung auf die Festplatte oder auf einem Videorekorder aufzeichnen. Auch die tageszeitabhängige Aufzeichnung mit Hilfe eines Schedulers ist vorgesehen. Für den Aufbau einer PC-gestützten Alarmzentrale wird die IP-Surveillance-Software mitgeliefert, die bis zu 16 Kameras gleichzeitig im Blickfeld haben kann. Für jede Kamera lassen sich individuelle Eigenschaften definieren – beispielsweise auch automatische E-Mails über die programmierten Ereignisse.

SEHR GELENKIG: Die W-LAN-Kamera DCS-5300W von D-Link schwenkt in alle Richtungen.

Kameraserie Mobotix M10D

Die Kameraserie M10 von Mobotix gehört zu den vielseitigsten Systemen im Bereich der Videoüberwachungstechnik.

Das Sortiment umfasst Kameras für den In- und Outdoor-Bereich. Letztere trotzen klimatischen Verhältnissen in einem Temperaturbereich von -20°C bis +65°C und sind dank des IP65-Gehäuses feuchtigkeitsresistent. Die Kamera ist mit einer Dual-Optik ausgestattet, die Weitwinkel- und Zoom-Aufnahmen von Details liefern kann.

Alternativ dazu gibt es für die Dual-Optik in der Ausführung „Night“ auch eine Infrarot-Optik. Damit sind auch bei schlechten Sichtverhältnissen gute Aufnahmen möglich.

Flexibel sind die Kommunikationsmöglichkeiten der M10D, denn die Kamera kann sowohl über eine IP-Netzwerk- als auch über eine ISDN-Wählverbindung angesteuert werden. Am Internet – an dieser Stelle werden IP-Adressen meist dynamisch zugewiesen – kann die aktuelle IP-Adresse telefonisch von einem synthetischen Sprachmodul der Kamera erfragt werden. Voraussetzung ist der ergänzende Anschluss der Kamera an das ISDN.

Mit Hilfe des integrierten Lautsprechers ist auch ein Dialog mit der beobachteten Person möglich.

OUTDOOR-GEEIGNET: Die Mobotix-Kameras sind fit für harte Außeneinsätze.

DER EXPERTEN-TIPP

Digitale Videoüberwachung setzt sich durch

Der digitalen Videoüberwachung gehört die Zukunft, der Anteil analoger Überwachungskameras wird immer weiter sinken. IMS Research prognostiziert für Netzwerkkameras bis 2008 eine jährliche Umsatzsteigerung von 28,4 Prozent im Bereich Europa, Mittlerer Osten, Afrika (EMEA).

Digital ist billiger **Die Gründe für diese Entwicklung sind ebenso zahlreich wie einleuchtend: Analoge Systeme sind aufgrund ihrer Abhängigkeit von Videokabeln weitgehend ortsgebunden, erfordern oft aufwendige Installationsarbeiten und sind dadurch meist deutlich teurer als digitale Systeme. Die bieten nicht nur mehr Funktionen wie etwa ereignisgesteuerte Aufnahmen und das automatische Auslösen von Alarmen per E-Mail oder Telefon, sie sind auch leicht und kostengünstig zu installieren, da sie über ISDN oder Ethernet-Kabel angeschlossen werden.**

Drahtlose Überwachung **Diese Datenkabel sind in den meisten modernen Gebäuden standardmäßig verlegt. Auch eine drahtlose Funkverbindung über W-LAN ist möglich, wodurch die Kameras große Außenareale überwachen können. Zu den generellen Vorteilen digitaler Überwachungstechnik bieten die Kameras von Mobotix weitere Pluspunkte: So sind alle Funktionen bereits in der Kamera integriert, was das Netzwerk schont, da die Kameras etwa Bilder zunächst intern speichern können und so keine ständige Verbindung zum Netzwerk benötigen. Zentral organisierte Kameras dagegen müssen ständig an einen PC angeschlossen sein.**

Autarke Bauweise **Durch ihre autarke Bauweise sind die Mobotix-Geräte vor Netzwerkausfällen geschützt, da sie Ausfallzeiten durch ihren internen Speicher überbrücken können. Angesichts dieser vielen Vorteile ist der Siegeszug der digitalen Videoüberwachung keine Überraschung.**

CHIP EXPERTE

Dr. Ralf Hinkel ist Vorstand und Gründer der Mobotix AG. Der Hersteller von wetterfesten Netzwerk-IP-Kameras entwickelt und produziert ISDN-/Netzwerk-Kameras für anwenderfreundliche Videoüberwachungs- und Webcam-Lösungen über IP-Netzwerke.

→ www.mobotix.de

ne Alarmzentrale übermitteln, dann muss die entsprechende Zielrufnummer definiert werden.

Drahtlose Überwachung mit E-Mail-Alarm

Dieses Einsatzszenario der Mobotix-Kamera scheint eine fest verdrahtete Umgebung vorauszusetzen, weil sich ihre vollen Funktionen nur dann nutzen lassen, wenn sowohl ein geeigneter Netzwerk- als auch ein ISDN-Anschluss verfügbar sind. Doch das Ganze lässt sich auch an entlegenen Stellen – etwa im Eingangsbereich großer Industrie- oder Privatgrundstücke – ohne Verkabelungsaufwand realisieren. So bieten verschiedene Hersteller Voice-over-IP-Gateways an, die ISDN-Basiskanäle über einen IP-Link schalten können, ohne dass direkt am Zielort ein ISDN-Anschluss vorhanden ist. Auch die Energieversorgung kann durch den Einsatz von Solarpanels und geeigneten Akkumulatoren rund um die Uhr sichergestellt werden. Dabei muss die Kamera nicht einmal in der unmittelbaren Nähe der übrigen Geräte positioniert werden, denn die Speisung des Gerätes ist sowohl über das Ethernet-Kabel als auch direkt über die ISDN-Schnittstelle möglich.

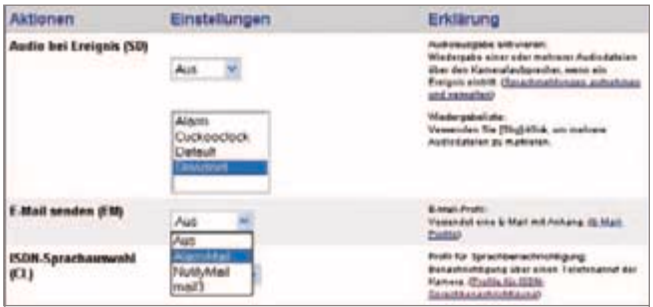
Natürlich ist auch mit diesem Modell eine permanente Überwachung des Objekts an einem Monitor-PC möglich, der durchaus mehrere Kameras in einer Multiview-Ansicht im Blickfeld behalten kann. Ereignisse werden in einer Event-Liste gespeichert und können auch später aus dem Speicher der Kamera (64 MByte) abgerufen werden. Alternativ ist auch die sofortige Benachrichtigung des Beobachters per E-Mail mit beigefügten Alarmaufnahmen der Kamera – beispielsweise im JPEG-Format – möglich.

Damit ein Alarm per E-Mail einschließlich eines ersten Beweisfotos gemeldet werden kann, sind verschiedene Konfigurationsschritte in der Kamera erforderlich: Zunächst einmal ist sicherzustellen, dass die Kamera einen E-Mail-Server kontaktieren kann. Dazu muss unter Umständen ein Internet-Zugang konfiguriert werden. Ist die Netzwerkanbindung hergestellt, erfolgt die Anmeldung am E-Mail-Server, wofür vom Administrator die üblichen Zugangsdaten (SMTP- und POP-Serveradresse, Benutzername, Kennwort und Absender-E-Mail-Adresse) bezogen werden müssen. In der globalen Konfiguration des E-Mail-Accounts der Kamera kann zudem die Struktur der Nachricht vorgegeben werden, wobei Mobotix eine Reihe von Variablen definiert hat. So lassen sich die Ereignisse konkret mit Datum, Uhrzeit und Kameraname in der E-Mail beschreiben.

Der Inhalt der E-Mail hängt von der Art des Ereignisses ab. Auch die Empfänger können variieren. Damit bei jedem Ereignis (Video-Bewegungsmelder, Infrarot-Melder etc.) eine individuelle E-Mail verschickt werden kann, lassen sich spezielle Profile definieren. Später wird im Setup-Menü die entsprechende Auswahl getroffen und die Benachrichtigung aktiviert.

Sobald die Kamera ein definiertes Ereignis bemerkt, verschickt sie automatisch eine elektronische Nachricht. Der Beobachter findet die Mail in seinem normalen Posteingang und kann anhand ihres Inhalts sofort entscheiden, ob er sich auf das Live-Bild der Kamera aufschalten möchte. Die dazu erforderliche IP-Adresse ist bereits in der Nachricht enthalten.

Robert Schoblick



ALARM PER E-MAIL: Einem bestimmten Ereignis – etwa der Reaktion des Video-Bewegungsmelders – wird eines der definierten E-Mail-Profile zugewiesen.

Funkareal prüfen

Die Planung im Vorfeld

Die Einrichtung eines W-LAN als Heimnetz ist heute kaum noch ein Problem. Bei professionellen Netzwerken, die hohe Performance und Teilnehmerzahlen sowie große Reichweiten vereinen sollen, sind dagegen gründliche Planung und ständiges Monitoring unerlässlich. Hier erfahren Sie, wie Sie einen Site Survey vornehmen.

Ein Wireless LAN basiert auf der Übertragung der Daten über Funkwellen, deren Frequenzen um 2,45 GHz beziehungsweise um 5 GHz definiert sind. Die Ausbreitung dieser Wellen ist nicht so einfach zu kontrollieren wie bei der Verwendung eines Kabels, denn sie können nicht nur an den gewünschten Standorten empfangen werden, sondern beeinflussen die gesamte Umgebung.

Das ist einerseits ein Vorteil, denn der Benutzer ist mit seinem Computer sehr flexibel in der Wahl seines Arbeitsplatzes und kann sich innerhalb des Sendebereichs nahezu völlig frei bewegen. Andererseits sind aber auch Nachteile mit der Ausbreitung von Funkwellen nach allen Richtungen verbunden. Das unkontrollierte Aussenden der Wellen stellt sowohl ein Sicherheitsrisiko dar als auch ein Hindernis für die optimale Performance des drahtlosen Netzwerks. Nicht zuletzt können auf der Funkstrecke Konfigurationsprobleme wirksam sein, die den Betrieb des bereits existierenden Netzwerks erheblich beeinträchtigen.

Um ein professionell genutztes drahtloses Netzwerk erfolgreich aufzubauen und zu betreiben, ist aus allen diesen Gründen eine gute Vorabplanung erforderlich mit dem Ziel, möglichst wenige Access Points installieren zu müssen. Darüber hinaus sollen auch die mobilen Endgeräte mit möglichst geringer Sendeleistung auskommen können, damit deren Akku geschont und eine optimale Betriebsdauer erreicht wird. Die Basis einer solchen, Site Survey genannten, Vorabplanung ist einerseits

die Analyse der Einflüsse möglicherweise bereits vorhandener drahtloser Netzwerke und andererseits

die Bewertung der dämpfenden Eigenschaften der Bausubstanz.

Während der Installationsarbeiten können regelmäßige Kontrollmessungen dazu genutzt werden, das Netzwerk noch in einem möglichst frühen Stadium zu optimieren. Nach Abschluss der Montagearbeiten eignen sich derartige Messungen für das Anlegen eines Abnahmeprotokolls. Regelmäßige Messungen der Feldstärken und Signal-Rauschabstände, aber auch Protokollanalysen gewährleisten die störungsfreie Betriebssicherheit des Funknetzes.

CHIP → DVD-CODE W-LAN

- **Gratis-Survey** Der Network Stumbler stöbert geschützte und ungeschützte W-LAN-Systeme auf, gibt Auskunft über SSID, MAC und AP-Hersteller und zeigt die Signalstärke an.
- **Profi-Analyse** Mit dem Laptop Analyzer erfassen Sie die Sendeleistung drahtloser Netze, finden mögliche Störquellen oder decken unauthorisierte Zugriffe auf Ihr W-LAN auf.

Abhörrisiken und Tempo-Bremsen ermitteln

Hohe Sendeleistungen der Access Points erscheinen auf den ersten Blick erstrebenswert, um möglichst ideale Leistungswerte mit dem W-LAN zu erreichen. Das ist unter der Voraussetzung, dass sich kein anderes Netzwerk in der Nähe befindet und dass mit einem einzigen Access Point eine sehr große Distanz zu überwinden ist, auch bedingt korrekt.

Die Realität sieht allerdings meist anders aus. In der Regel werden in unmittelbarer Nachbarschaft weitere drahtlose Netze zu finden sein, die alle unter dem Aspekt der optimalen Leistung in Betrieb genommen wurden und mit großer Wahrscheinlichkeit mit dem Maximum an verfügbarer Sendeleistung arbeiten. Das Problem besteht nun darin, dass nur eine sehr begrenzte Anzahl von Kanälen verfügbar ist.

Die Anzahl der Kanäle ist übrigens nicht mit der der zugelassenen Funkkanäle gleichzusetzen, denn infolge der Bandspreizungsverfahren, die bei W-LAN zum Einsatz kommen, erstreckt sich ein W-LAN-Kanal stets über mehrere Funkkanäle. Arbeiten zwei Netze unmittelbar nebeneinander auf vollkommen verschiedenen Kanälen, steht ihnen unabhängig vom direkten Nachbarn die volle Kapazität zur Verfügung. Arbeiten dagegen beide Netze auf dem gleichen oder einem unmittelbar benachbarten Kanal – das ist möglich und häufig auch üblich – müssen sie sich die verfügbaren Ressourcen teilen. Jedes einzelne Netz wird dann erheblich langsamer!

Es ist übrigens – abgesehen von der Performance-Einschränkung – kein Problem, zwei W-LANs auf dem gleichen Funkkanal in der unmittelbaren Nachbarschaft zu betreiben, weil sich die Geräte anhand des Service Set Identifiers (SSID) erkennen. Allerdings – auch das kommt häufig vor – übernehmen insbesondere im privaten Nutzungsbereich viele W-LAN-Betreiber leichtsinnigerweise die Standard-Einstellungen des Herstellers. Arbeiten diese Netze dann auch noch mit einer automatischen Vergabe der IP-Adressen über den DHCP-Service, dann findet sich der eine oder andere Benutzer plötzlich in einem fremden Netzwerk wieder. Mit einer Protokollanalyse lassen sich auch an dieser Stelle schnell Klarheiten schaffen und offene W-LANs in der Umgebung, aber auch eigene Sicherheitslücken erkennen.

Die versehentliche Anmeldung in einem völlig fremden Netzwerk infolge schlechter Konfiguration des Netzes und fehlender Kenntnis der Verhältnisse in der funktechnischen Nachbarschaft sind ein Problem für sich. Ein anderes Problem

Die besten Site-Survey-Tipps im Web

Tom's Hardware → www.tomshardware.de/network/20040624/ Testbericht des Ekahau-Site-Survey-Tools
Praxisbeispiel I → www.hpgmbh.de/produktseiten/details/wlan_dienst.html Übersicht zu den Schritten eines Site Surveys
Praxisbeispiel II → www.konvergenzforum.de/Werkzeuge_zur_WLAN_Planung.pdf Darstellung eines Site Surveys
Profi-Werkzeuge → www.airmagnet.com Informationen zum Surveyor und Laptop Analyzer

sind vorsätzlich handelnde Angreifer – so genannte War-Driver –, die gezielt ungeschützte Netze suchen, um über diese einen kostenlosen und vor allem anonymen Weg ins Internet zu finden oder die Gunst der Stunde zu nutzen, ihre Opfer massiv zu sabotieren (lesen Sie dazu das Special ab 68).

Diesen War-Drivern macht man die Angriffe nur allzu leicht, wenn die eigene Sendeleistung sehr hoch gewählt wird. Weil War-Driver oft mit Richtantennen arbeiten, die in ihrer Hauptstrahlrichtung einen sehr guten Gewinn haben, stehen ihnen somit selbst bei weiten Entfernungen zum Access Point noch nahezu ideale Bedingungen zur Verfügung. Je geringer aber die nach außen dringende Sendeleistung ist, desto schwieriger wird ein erfolgreicher Angriff. Für Netzwerke, deren Betreiber sehr hohe Sicherheitsanforderungen haben, gehören deshalb unmittelbar nach der Inbetriebnahme Outdoor-Messungen zur Pflicht. Solche Messungen sollten sie in regelmäßigen Abständen wiederholen – insbesondere dann, wenn sich an der Gestaltung der Infrastruktur etwas verändert hat.

Umfeld des W-LAN genau inspizieren

Die professionelle Planung eines komplexen W-LAN-Systems beginnt am Standort des Netzwerks. Das erweist sich auch dann als sinnvoll, wenn das mit W-LAN zu versorgende Gebäude noch gar nicht steht, denn der Planer kann sich auf diese Weise einen Überblick über die Beschaffenheit der Umgebung verschaffen. Diese Eindrücke sind wichtig, um eventuelle Beeinflussungen des Netzes durch benachbarte Systeme abschätzen zu können. So ist etwa zur Versorgung eines Campus-Geländes oder zur Einrichtung eines W-LAN-Hotspots in einem weiträumigen Biergarten auch die Vegetation von Bedeutung. Wird das Netzwerk im Winter errichtet, weil in dieser Zeit der Biergarten geschlossen ist und die Montagearbeiten den Betrieb nicht stören, liefern die Messungen in dieser Zeit bessere Ergebnisse, als dies im Sommer der Fall ist, wenn Bäume und Sträucher mit Blättern bedeckt sind. Innerhalb von Gebäuden sind die Bausubstanz und die Art der Wandverkleidung ebenfalls wichtige Kriterien für die Planung des Funknetzes. So haben metallische Flächen, wie sie in Bauwerken mit einer sehr modernen Architektur zum Einsatz kommen, durchaus abschirmende Wirkungen. Sie können aber auch Funksignale reflektieren und damit eine kalkulierte Richtwirkung der verwendeten Antenne beeinträchtigen. Ein Ortstermin verschafft dem Experten auf einen Blick die nötigen Informationen, die er in die weitere Planung des W-LANs einbeziehen kann.

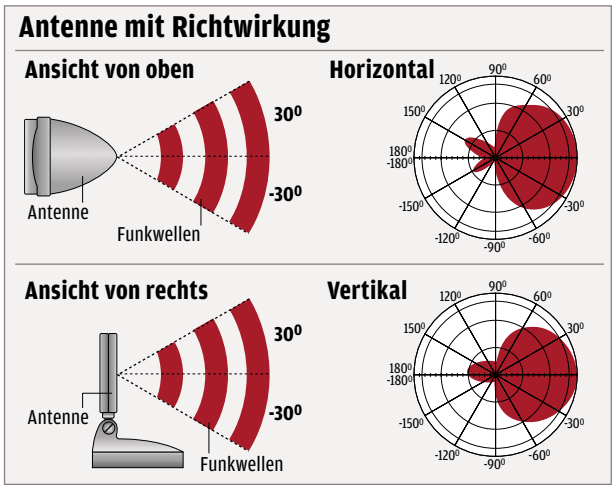
In einem Bürogebäude, in dem davon auszugehen ist, dass mehrere drahtlose Netze auf engstem Raum betrieben werden, ist ein Ortstermin eine gute Gelegenheit für den Planer, mit den technisch Verantwortlichen der unmittelbaren Nachbarn zu sprechen. Da benachbarte W-LANs einander in ihrer Leistungsfähigkeit beeinträchtigen können, ist ein Dialog im Interesse aller Beteiligten wichtig. Insbesondere sind zu diskutieren, wie hoch die Sendeleistungen der Netzwerke sind und welche Kanäle in den Netzsegmenten verwendet werden, die die Grenzen der eigenen Räume überragen.

Ganz wichtig für die Planung des Funknetzes ist es, den Grundriss eines Gebäudes zu berücksichtigen, wobei auch die Etagen ober- und unterhalb des zu versorgenden Stockwerks eine Rolle spielen. Anhand der Beobachtungen beim Ortstermin →

PROFI-TIPP

Sendeleistung reduzieren

Gerade wenn größere Netzwerke eingerichtet werden sollen, die zwei Bedingungen – hohe Nutzerzahl und hohe Performance – vereinen müssen, erweist sich eine geringe Sendeleistung der Geräte als Segen. **Kleinzellige Netze** Wegen der damit verbundenen geringen Sendereichweite kann der verwendete Kanal schon nach weniger als zehn Metern – theoretisch sogar schon im Nebenraum – erneut für ein W-LAN verwendet werden. Pro Access Point arbeiten also nur sehr wenige Benutzer im Netzwerk, wodurch ihnen jeweils die optimale Airtime zur Verfügung steht. Die Sendeleistung lässt sich durch eine entsprechende Konfiguration des Access Points beeinflussen. Es empfiehlt sich deshalb, sie so niedrig einzustellen, dass an den Arbeitsplätzen gerade noch die ideale Geschwindigkeit genutzt werden kann. **Antenne mit Richtwirkung** Funkkanäle lassen sich in einer kurzen Distanz zwischen den Access Points mehrfach verwenden, wenn eine Antenne mit starker Richtwirkung zum Einsatz kommt. Eine solche Antenne fokussiert ihre Sende- und Empfangseigenschaften auf W-LAN-Geräte, die sich in ihrer Hauptstrahlrichtung befinden. Mit solchen Richtantennen und minimal eingestellter Sendeleistung lassen sich sehr kleinzellige W-LANs aufbauen, die einer hohen Benutzerzahl den gleichzeitigen Netzwerkzugang gestatten, ohne dabei in der Geschwindigkeit einzubrechen.



GUT AUSGERICHTET: Horizontal und vertikal bietet diese Antenne in einem Winkel von +/- 30° die besten Eigenschaften. In einem Gebäude können die verwendeten Kanäle auch in den angrenzenden Stockwerken genutzt werden.

Illustration: CHIP S. Schönberger

PROFI-TIPP

Site Survey fürs kleine W-LAN

Eine professionelle Diagnosesoftware wie die im Beitrag vorgestellten Programme Laptop Wireless LAN Analyzer oder Surveyor von Airmagnet kosten zwischen 2.000 und mehr als 3.000 Dollar. Für eine präzise Planung und Dokumentation der Ergebnisse ist eine solche Software für Profis unerlässlich.

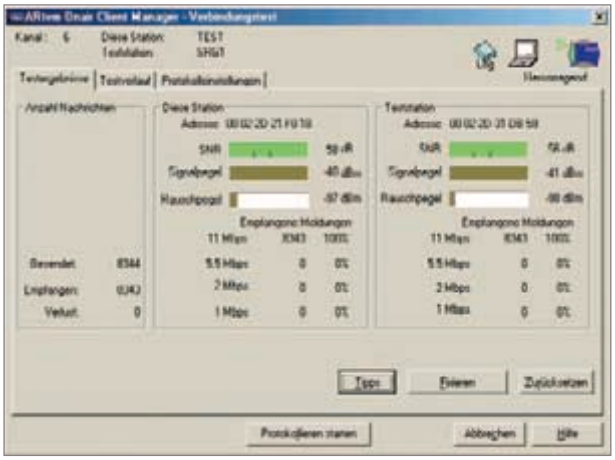
Wer jedoch im kleinen Stil – beispielsweise gemeinsam mit seinen Nachbarn im Haus – die Leistungsfähigkeit drahtloser Netze verbessern möchte, kann auch auf die Funktionen zurückgreifen, die viele Anbieter bereits mit ihren W-LAN-Karten liefern. Ein solches Programm – etwa der ARtem-Onair-Client-Manager – liefert bereits sehr interessante Daten für die Auswahl des günstigsten Montage-Ortes für einen Access Point.

Was der SNR aussagt **Der Signal-Rauschabstand (SNR) gibt beispielsweise an, wie gut das eigentliche Nutzsignal über dem Störsignalpegel liegt. Je größer dieser Wert ist, um so besser ist die Verbindung. Die absichtliche Reduktion von Sendeleistung hat jedoch einen direkten Einfluss auf diesen Wert. Es sollte also nicht allein ein möglichst hoher SNR-Wert, sondern eine ideale Performance angestrebt werden. An dieser Stelle erweist sich die Auswertung der Testdaten als ein guter Weg.**

Im Beispiel wurden 8.344 Testpakete verschickt, 8.343 wurden störungsfrei empfangen, bei einem Paket steht das Ergebnis noch aus. Eine der wichtigsten Informationen ist allerdings, dass alle Testdaten mit einer Brutto- Geschwindigkeit von 11 MBit/s übermittelt werden. Das Netz arbeitet also unter optimalen Bedingungen.

Test im Nebenraum **Bewegt man nun das Notebook in einem anderen Raum, kann man prüfen, ob auch an dieser Stelle noch gute Werte erreicht werden. Um möglichst zeitnah zu testen, wie sich die Veränderung eines Standorts auswirkt, kann man auf eine grafische Darstellung umschalten. Dabei lassen sich sehr gut die tendenziellen Veränderungen erkennen. Doch Vorsicht: Jedes digitale Mess-System benötigt eine gewisse Torzeit, in der die Daten erfasst und ausgewertet werden. Gute Ergebnisse werden erzielt, wenn man die Ortsveränderungen sehr langsam vollzieht.**

Die Ergebnisse lassen sich allerdings auch leicht verfälschen! Decken Sie beispielsweise die Antenne der W-LAN-Karte des Notebooks mit der Hand ab, messen Sie bis zu zweistellig schlechtere dB-Werte als bei einer frei im Raum bewegten Antenne.



SIGNAL-RAUSCHABSTAND: Möglichst viel Abstand zwischen Nutzsignalpegel und Rauschpegel ist eine wichtige Voraussetzung für ein störungsfreies Netzwerk.

werden Art und Beschaffenheit der Bausubstanz in diesem Grundriss notiert und darüber hinaus die Einwirkung von benachbarten Netzen vermerkt. Zu den an dieser Stelle interessanten Daten gehören die SSID und die Betreiber der jeweiligen Funknetze, die Kanäle, auf denen die benachbarten Netze arbeiten und die gemessene Signalstärke.

Kanal- und Funkzellenplanung vornehmen

Während in drahtgebundenen Netzwerken das Prinzip der Kollisionserkennung (CSMA/CD) die dezentrale Zugriffssteuerung der einzelnen Computer auf das Medium bestimmt, arbeiten W-LANs nach dem Prinzip der Kollisionsvermeidung (CSMA/CA). Daher sind entsprechende Dialoge und Wartezeiten definiert, in denen keinerlei Daten übertragen werden können. Je größer die Anzahl der W-LAN-Geräte innerhalb eines Sendebereichs und Funkkanals ist, um so größer wird der Einfluss der Wartezeiten und um so kleiner wird insgesamt der durchschnittliche Anteil an der verfügbaren Airtime für jeden einzelnen Computer. Die Konsequenz: Je mehr Rechner innerhalb eines W-LAN-Sendebereichs betrieben werden, um so geringer ist die Performance des Wireless-Netzes für jeden einzelnen Computer.

Wichtig ist dabei, dass sich diese Betrachtung bereits auf die physikalische Schicht bezieht, also noch keinerlei Definitionen einer SSID oder ähnliches eine Rolle spielen. Benachbarte Netze, die sich in ihrer SSID aus der Sicht der Anwendung klar voneinander trennen lassen, jedoch auf dem gleichen Kanal arbeiten, sind unter der Betrachtung der physikalischen Schicht ein W-LAN, dessen Komponenten sich die verfügbaren Ressourcen teilen müssen.

Will man einer großen Anzahl von Computern den zeitgleichen Zugang zum Netzwerk ermöglichen, muss man das Funknetz – wie auch bei drahtgebundenen Netzen durchaus üblich – segmentieren. Wegen der sehr eingeschränkten Möglichkeiten, die Ausbreitung der Funkwellen zu begrenzen, ist dies nur möglich, wenn

die verfügbaren Funkkanäle sinnvoll ausgenutzt werden,
Antennen mit guter Richtwirkung zum Einsatz kommen, und
die Sendeleistung der Geräte so weit reduziert wird, dass gerade noch die gewünschte Performance innerhalb des definierten örtlichen Umfelds erreicht wird.

Ziel ist es also – ähnlich wie im öffentlichen Mobilfunk –, möglichst kleinzellige Netze zu schaffen, die einer möglichst großen Zahl von Benutzern erlauben, gleichzeitig mit optimaler Performance im Netz zu agieren.

Die Reduzierung der Sendeleistung erlaubt es, möglicherweise bereits nach wenigen Metern den verwendeten Kanal erneut einem anderen Netzwerksegment zuzuweisen, ohne dass eine gegenseitige Beeinträchtigung stattfindet. Durch den Einsatz von Antennen mit starker Richtwirkung ist es zudem möglich, auf sehr engem Raum die Benutzerzahl zu erhöhen.

Generell ist es jedoch problematisch, so definierte Zellen unter Verwendung des gleichen Kanals unmittelbar nebeneinander zu betreiben, da sich die Bereiche bei lückenloser Versorgung zwangsläufig überschneiden. Aus diesem Grund sollten direkt benachbarte W-LAN-Sendebereiche auf unterschiedlichen Kanälen arbeiten. Mit Hilfe von Feldstärkemessungen

DER EXPERTEN-TIPP

Site Surveys regelmäßig vornehmen

Jeder professionelle W-LAN-Site-Betreiber sollte vor der Installation und Inbetriebnahme exakte Site Surveys durchführen. Zum einen lässt sich damit die gewünschte Funkausleuchtung überprüfen, und zum anderen entdeckt man mit dem Site Survey benachbarte W-LAN-Installationen und andere Störquellen.

Viele Nutzer, volle Kanäle Die W-LAN-Installationen nehmen zu. Denn sowohl beim Heimanwender als auch in der Industrie wird Wireless LAN immer häufiger eingesetzt. Täglich entstehen mehr Hotspots für den mobilen Internet-Zugang, Verkehrsüberwachungskameras werden per W-LAN vernetzt, Verkehrsbetriebe nutzen W-LAN für Fahrgastinformationssysteme und in Krankenhäusern werden mobile Terminals zur Patientendatenerfassung eingesetzt. Alle diese Nutzer müssen sich das kleine, lizenzfreie 2,4-GHz-ISM-Band teilen, in dem für W-LAN nur drei Kanäle zur Verfügung stehen, die sich nicht gegenseitig beeinflussen.

Home-Entertainment per W-LAN Auch immer mehr Home-Entertainment-Systeme nutzen das ISM-Band, um Audio- und Videosignale zu übertragen. Diese Geräte arbeiten meist mit einer relativ hohen Sendeleistung sowie hohen Verkehrslasten und stören daher W-LAN-Installationen in ihrer Umgebung sehr stark.

Regelmäßig prüfen Um den Betrieb eines W-LANs sicherzustellen, muss der Betreiber immer wieder Site Surveys durchführen und auf veränderte Umgebungsbedingungen reagieren. Dazu eignet sich zum Beispiel der AirMagnet Surveyor Professional. Mit diesem Tool lassen sich die Messergebnisse grafisch in den hinterlegten Kartendaten darstellen, Simulationen durchführen und ausführliche Reports anlegen. Neben den regelmäßigen Site Surveys ist auch eine ständige Überwachung des Funknetzwerks ratsam. Denn nur so kann der Betreiber auf Störungen reagieren, bevor der User sie überhaupt bemerkt.

CHIP EXPERTE

Christian Gauer ist als Leiter Technik beim IT-Lösungsanbieter DDS GmbH, München, auch für den Bereich Wireless LAN verantwortlich. Die DDS GmbH vertreibt nicht nur Lösungen im Netzwerkbereich, sondern entwickelt auch Analyse-, Monitoring- und Troubleshooting-Lösungen und sowie Projekte für W-LANs.

→ www.ddsgmbh.de

an verschiedenen Stellen des Raumes lassen sich die Grenzen der Zellen ermitteln und durch Nachjustierung der Antennen beziehungsweise der Sendeleistung optimieren.

W-LAN professionell analysieren

Professionelle W-LAN-Analysen beginnen bereits im Vorfeld der Einrichtung eines drahtlosen Netzwerks und enden nicht mit dessen Inbetriebnahme. W-LAN-Analyzer kommen weiterhin zur Optimierung der Performance, zur Fehlerdiagnose und auch zur Lokalisierung von Sicherheitslücken zum Einsatz. Ein solches Diagnosewerkzeug bietet das amerikanische Softwarehaus AirMagnet mit dem Laptop Wireless LAN Analyzer an. Da es sich um eine Diagnose-Software handelt, ist eine bestimmte – vom Hersteller vorgesehene – W-LAN-Hardware Voraussetzung für die Funktion und Präzision des Programms.

W-LAN-ANALYSE: Zwar wird lediglich ein Kanal im gesamten W-LAN-Spektrum benutzt, der ist aber von zwei verschiedenen Netzen belegt. Die Betreiber beider Netze verzichten so auf die optimale Performance ihrer Systeme.

Bevor ein neues Netzwerk errichtet wird, ist der erste Schritt die Erkundung der Umgebung. So wird festgestellt, wie viele und welche benachbarten Netze vorhanden sind und auf welchen Kanälen sie arbeiten. Es interessieren aber nicht nur die W-LANs nach IEEE 802.11a/b/g, sondern auch alle anderen Störeinflüsse, die auf den verfügbaren Kanälen messbar sind.

Das so genannte Rauschen (Noise) kann seine Ursprünge haben in atmosphärischen Störungen, in Reflexionen und Einstrahlungen anderer, weit entfernter Signalquellen und in Oberwellen von Sendern, die regulär auf einem anderen Frequenzband betrieben werden. Da die ISM-Bänder (siehe 16) jedoch für viele Anwendungen offen sind, haben auch andere Geräte, etwa ein Mikrowellenofen oder ein Bluetooth-System, direkten Einfluss auf den Störsignalpegel.

Das Rauschen ist nicht auf allen Kanälen gleich stark. Daher ist diese Größe ein weiteres Kriterium für die Auswahl des Betriebskanals für das eigene System. Generell gilt, dass der Noise-Pegel (in dB) möglichst gering sein soll (im Beispiel links liegt er bei -92 dBm). Weitaus wichtiger ist jedoch der Abstand des Nutzsignals vom Störsignal. Die beiden in diesem Beispiel gefundenen Signale haben einen Abstand zum Rauschpegel von 47 dB beziehungsweise 52 dB – ideale Werte.

Die erste Analyse bringt bereits wichtige Entscheidungsargumente. So ist in diesem Beispiel zu erkennen, dass das gesamte 5-GHz-Band in den für IEEE 802.11a definierten Kanälen noch vollkommen unbelegt ist. Im 11b-Bereich drängen sich dagegen bereits zwei Netzwerke auf dem Kanal 6, der damit für die eigene Belegung ausscheidet. Um Beeinträchtigungen durch die Effekte der Bandspreizung zu vermeiden, wählt man anhand dieser Ergebnisse nun einen Betriebskanal, der einen Abstand von zwei Kanälen zu den stärksten Nachbarnetzen hat. Die Kanäle 3 und 9 würden sich also für ein 11b-Netzwerk anbieten.

Natürlich ist das gezeigte Beispiel funktechnisch eine nahezu ideale Umgebung, denn es wurden nur zwei Netze gefunden, →

die noch dazu auf einem Kanal liegen. In dichter besiedelten Arealen ist ein vollkommen freier Kanal eher mit einem Lottogewinn gleichzusetzen.

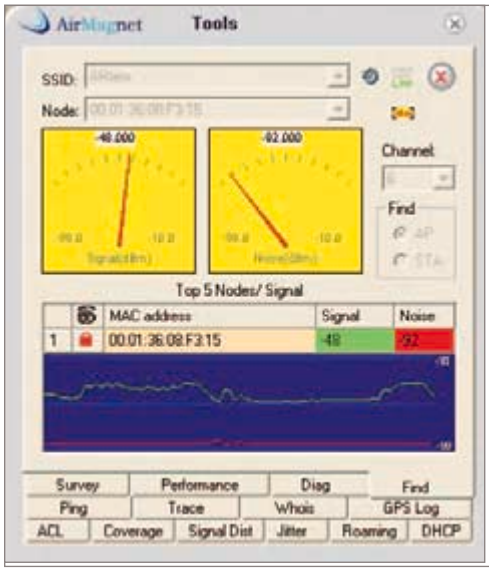
Doch anhand der Signalstärken lassen sich die Netze in der unmittelbaren Umgebung ermitteln. Oft kann auf der Basis dieser Ergebnisse ein Gespräch mit dem Nachbarn dazu führen, dass alle W-LAN-Betreiber ihr Netz mit optimaler Performance nutzen können, wenn die Sendeleistung jeweils angepasst wird.

Messungen der Signalstärke des eigenen Access Points, der Stärke der benachbarten Netze und des Signal-Rauschabstands sollten an allen wichtigen Stellen innerhalb der eigenen Räumlichkeiten vorgenommen und die Ergebnisse in einem Grundriss erfasst werden.

Nach einer allgemeinen Übersicht über alle Kanäle können die Vorgänge auf den einzelnen Kanälen im Detail betrachtet werden. So lässt sich die Anzahl der Access Points und der Client-Stationen innerhalb des Empfangsbereichs feststellen. Wer ein größeres Wireless LAN betreibt, das aus mehreren vernetzten Access Points besteht, kann anhand dieser Ergebnisse möglicherweise die Anzahl der Client-Stationen und deren Position optimieren.

Netzlast ausgewogen verteilen

Handlungsbedarf besteht beispielsweise, wenn an einem Access Point wesentlich mehr Clients angemeldet sind als an den übrigen Knoten. An dieser Stelle wird eindeutig Performance verschenkt, denn die meisten Access Points sind nicht ausgelastet, während sich in einem Sendebereich sehr viele Computer um die Belegung des Kanals bemühen. Regelmäßige Analysen der im W-LAN befindlichen Client-Computer können auch Angriffsversuche aufdecken. Denn War-Driver, die in das Netz eindringen wollen, hinterlassen anhand der MAC-Adresse ihrer W-LAN-Karte eindeutige Spuren.



MESSINSTRUMENT: Aussagefähige Daten und eine schnelle Tendenzanzeige sind für ein Site Survey sehr sinnvoll, etwa um Dämpfungssituationen für Antennen-Positionen zu erfassen.

Verschiedene Tools können den Aufbau eines Netzwerks und die Diagnose in bestehenden Systemen stark vereinfachen. Um bei einem Site Survey möglichst schnell die tendenziellen Folgen einer Veränderung im System erkennen zu können, sind eigentlich analoge Messinstrumente erforderlich. An diesen Geräten lässt sich am sofort reagierenden Zeigerausschlag erkennen, ob etwa die Ausrichtung einer Antenne positive oder negative Einflüsse auf das System hat.

Ein kleines Software-Tool, das ein solches Zeigerinstrument simuliert (siehe Abbildung oben), benötigt extrem geringe Torzeiten und kann deshalb nicht ganz an die Genauigkeit der zuvor gezeigten Verfahren zur Messung von Signalstärke und des Signal-Rauschabstands herankommen. Dafür reagiert ein solches Tool sehr spontan, was in diesem Beispiel durch Umfassen

KNOW-HOW

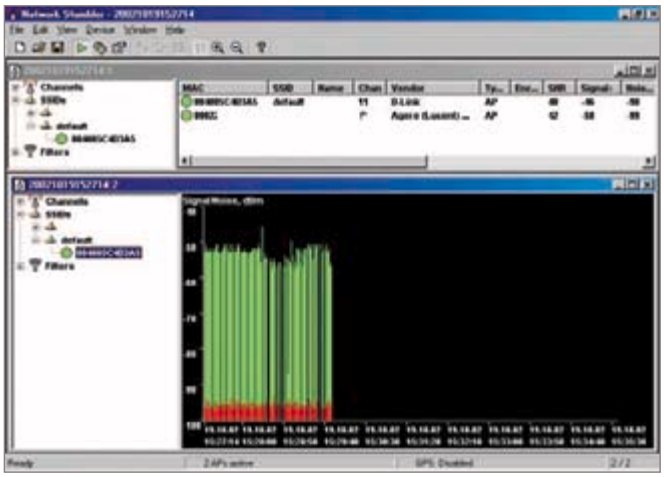
War-Driver nutzen am liebsten Analyse-Software

Was der Netzwerk-Administrator oder der Servicetechniker mit einem geeigneten Diagnoseprogramm tun kann, das können auch War-Driver und W-LAN-Hacker. Im Internet gibt es zahllose Programme, mit deren Hilfe ungeschützte W-LANs problemlos aufgespürt werden können.

Bordmittel reichen **Im Prinzip genügen für diesen Zweck sogar die Bordmittel der W-LAN-Karte, die vom Hersteller mitgeliefert werden. Selbst Software, mit deren Hilfe WEP-Schlüssel geknackt werden können, ist ohne weiteres im Internet zu finden.**

Risiko W-LAN-Einbruch **Durch den ungehinderten Zugang zu den Netz-Laufwerken kann ein Angreifer in den Besitz vertraulicher Dokumente und Passwörter kommen. Ebenso kann sich ein Hacker Zugang zum Internet verschaffen und damit unter falscher Identität surfen oder sogar kriminellen Aktivitäten nachgehen. Alle wichtigen Informationen kann ein gut ausgestatteter Hacker aus der Aufzeichnung der bitgenauen Protokolldaten in Erfahrung bringen.**

Warnung vor Schwachstellen **Diagnose- und Analyse-Tools sind also nicht nur Hilfsmittel zum Auffinden einer Störung. Sie sind ebensosehr als Warnung vor Schwachstellen und eindringliche Ermahnung zur gründlichen Absicherung des drahtlosen Netzwerkes zu verstehen.**



ZWEISCHNEIDIG: Der Network Stumbler ist ein Site-Survey-Tool, das im Internet frei verfügbar ist. Allerdings nutzen es auch War-Driver gerne, um ungesicherte Netze aufzuspüren.

der W-LAN-Antenne mit der Hand simuliert wurde. Mikrowellen werden durch Wasser absorbiert und weil der menschliche Körper überwiegend aus Wasser besteht, dämpft das Umschließen der Antenne mit der Hand das Signal, was deutlich messbar und aufgrund der Reaktionszeit der Anzeige überprüfbar ist.

Site Survey im laufenden Betrieb

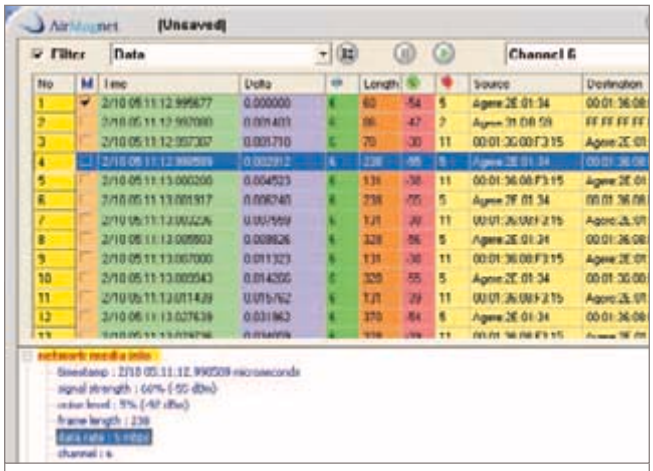
Ist das Netzwerk einmal aufgebaut, gibt es insbesondere in drahtlosen Netzen immer wieder Klagen über die Geschwindigkeit – vor allem über das Missverhältnis zwischen den vermeintlichen Nenngeschwindigkeiten und dem tatsächlichen Tempo des Netzwerks. Eine gute Statistik zum Verhältnis der Übertragung von Paketen in verschiedenen Geschwindigkeitsstufen macht schnell deutlich, ob in dem System häufig auf geringere Geschwindigkeiten zurückgeschaltet wird, sodass Handlungsbedarf bestehen würde.

Probleme durch ungünstiges Routing oder allgemein zu lange Laufzeiten im Netzwerk werden dadurch aber nicht erkannt. An dieser Stelle kann ein einfacher Echo-Request (mit ping) bereits Klarheit bringen. Darüber hinaus lässt sich anhand der Visualisierung aller Knoten (mit trace-route) ungünstiges Routing erkennen (mehr zu Diagnose-Tools lesen Sie ab 122).

An dieser Stelle wird schnell deutlich, dass eine Störungsdiagnose in einem W-LAN weder allein auf die Funkschnittstelle beschränkt bleiben darf, noch ausschließlich mit klassischen Diagnose-Tools betrieben werden sollte. Nur eine vollständige Betrachtung der Situation kann zuverlässige Ergebnisse bringen.

Detaillierte Protokoll-Analysen starten

Eine Reihe dieser Analysen lassen sich mit „Bordmitteln“ der W-LAN-Karten oder mit anderen Programmen, etwa dem Network Stumbler (auf Heft-DVD) durchführen. Problematisch wird es jedoch, wenn Verbindungsprobleme im Detail



PROTOKOLL-ANALYSE: Die Decodierung der Frames beginnt auf der physikalischen Ebene und ermittelt für jeden Frame Signalstärke, Störsignalpegel, Kanal und Burstgeschwindigkeit.

untersucht werden müssen. An dieser Stelle sind nicht nur konkrete Kenntnisse der Netzwerktechnik in allen Protokollschichten – auch denen unterhalb der IP-Ebene – erforderlich, sondern auch ein bit-genaues Diagnose-Werkzeug. Eine solche Protokoll-Analyse ist extrem aufwendig, sodass es sehr wichtig ist, Filter setzen zu können. Wer eine solche Analyse vornimmt, weiß in der Regel, wonach er sucht, und kann die Anzeige somit auf das Wesentliche beschränken.

Ein großer Fehler wäre es etwa – es sei denn, man möchte gezielt diese Funktion untersuchen – die „Leuchtfeuer“-Signale (Beacon) der Access Points zu tracen. Dort wird innerhalb kürzester Zeit eine exorbitant lange Liste von Ereignissen aufgezeichnet. Diesen Parameter sollte man also generell ausklammern, um nicht die Übersicht zu verlieren. Robert Schoblick

KNOW-HOW

Dezibel – „Einheit“ und doch keine Maßeinheit

Antennen werden mit ihrem Gewinn, der Einfluss der Umgebung durch die Dämpfung, definiert. Darüber hinaus berücksichtigt man bei der Planung von W-LANs und bei der Diagnose im Fehlerfall den Störsignalpegel sowie den Abstand des Nutzsignals vom Störsignal. Die Angaben dieser Größen erfolgen als relative Werte ohne echte Maßeinheit und werden in Dezibel (dB) dargestellt.

Bezugsgröße für dB-Wert Da ein dB-Wert immer eine relative Größe ist, muss es also stets eine Bezugsgröße geben. Für den Antennengewinn ist diese Bezugsgröße entweder der so genannte isotrope Kugelstrahler, eine ideale, aber nicht praktisch zu bauende Antenne, die nach allen Richtungen die gleichen Strahlungseigenschaften aufweist, oder der Halbwellendipol, der als die einfachste realisierbare Antennenbauform und deshalb als Elementarantenne gilt. Der Halbwellendipol hat nicht die gleichen Eigenschaften wie die ideale Antenne und somit gegenüber dem isotropen Kugelstrahler bereits einen Gewinn von 2,15 dB.

Relativer Gewinn Gibt man den Antennengewinn gegenüber dem Halbwellendipol an, spricht man vom relativen Gewinn in der Einheit dB. Soll der Gewinn jedoch im Verhältnis zur idealen Antenne definiert werden, so spricht man vom absoluten oder isotopen Gewinn. Die Einheit wird um einen darauf hinweisenden Zusatz, nämlich „i“, erweitert: dBi.

Logarithmische Darstellungen Angaben in dB sind logarithmische Darstellungen der Verhältnisse. Da es sich beim Antennengewinn um das Verhältnis von Leistungswerten handelt, gilt die folgende Beziehung:

G = 10* log (P/Pref)

Pref soll die Referenzgröße, also entweder der isotrope Kugelstrahler oder der Halbwellendipol sein, P entspricht der Leistungsangabe für die Antenne. Hätte die Antenne etwa die doppelte Strahlungsleistung wie die Referenzantenne, dann wäre der Gewinn:

G = 10*log (2)

G = 3 dB

Somit wäre ein Gewinn von 6 dB eine Vervierfachung der Leistung. Dämpfungswerte gibt man dagegen mit negativen Vorzeichen an. Wählt man anstelle einer Referenzantenne einen definierten Bezugswert von 1 mW, dann wird dies in der „Einheit“ durch den Zusatz „m“ angegeben. Bei einer Referenz zu 1 mW spricht man also von dBm. Ein Wert von 3 dBm entspricht einer absoluten Leistungsangabe von 2 mW, und 30 dBm entsprechen einer Leistung von 1 W.

Logarithmische Spannungs- und Stromverhältnisse werden anstatt mit dem Faktor 10 mit dem Faktor 20 ausgedrückt. Eine Verdopplung eines Spannungswertes entspricht also 6 dB.

Begehrter Kunden-Service

W-LAN-Hotspot einrichten

In Top-Hotels, großen Bahnhöfen und auf Flughäfen ist es schon selbstverständlich, mit dem Notebook über einen W-LAN-Hotspot drahtlos im Internet surfen zu können. Aber auch kleinere Hotels, Pensionen oder andere Unternehmen können ihren Kunden einen Hotspot anbieten, ohne dabei ihr Kerngeschäft aus den Augen zu verlieren.

Öffentliche Wireless-LAN-Zugänge – so genannte Hotspots – schießen in exklusiven Locations wie Top-Hotels und Flughäfen wie die Pilze aus dem Boden. Sowohl diese Exklusivität als auch die Anforderungsprofile an einen Hotspot schrecken allerdings häufig eine Zielgruppe davon ab, die neben den Umsätzen aus dem Verkauf von Online-Zeit auch verschiedene andere Vorteile aus dem Betrieb eines W-LAN-Hotspots für sich nutzen könnte: Kleine und mittelständische Unternehmen – vorzugsweise aus dem Bereich der Gastronomie und dem Hotelgewerbe – können ihren Kunden mit einem W-LAN-Hotspot einen attraktiven Mehrwert bieten und damit indirekt auch das Kerngeschäft positiv beeinflussen.

Aus Sicht des Benutzers ist ein W-LAN-Hotspot ein öffentlich zugängliches, drahtloses Netzwerk, das mit einem oder mehreren vernetzten Access Points aufgebaut ist. Um das Netzwerk nutzen zu können, muss sich der Benutzer jedoch zunächst am System anmelden. Erst dann können wirklich alle Angebote – einschließlich des Internet-Zugang – genutzt werden. Dieser Zugang zum Internet ist der eigentliche Zweck eines Hotspots, der – anders als in einem Internet-Café – über den persönlichen Computer oder PDA des Benutzers ermöglicht wird. Das hat auch sicherheitstechnische Vorteile.

Der Betreiber des Hotspots kann Online-Zeiten, aber auch Werbeflächen verkaufen. Dazu verwendet er Voucher, entweder als „Rubbelkarte“ oder als einfacher Computerausdruck. Die Form der Abrechnung bestimmt das System. So gibt es Lösungen, bei denen spezielle Dienstleister die Abrechnung vornehmen, und solche, bei denen der Betreiber eigene Voucher herstellen und damit auch seine Tarife frei festlegen kann.

COMPASS: Die Zentrale des gesamten Hotspots ist der Access-Server (ComPass). Er stellt die abgerufenen Webseiten bereit und verwaltet die Benutzerkonten.

KNOW-HOW

Wichtige Hotspot-Begriffe

Walled Garden: Kostenlos in einem Hotspot zugänglicher Bereich. Er kann auch ohne vorherige Anmeldung mit den Benutzerdaten eines zuvor gekauften Vouchers besucht werden.

Landing Page: Startseite des Hotspots. Gute Hotspots sind so konfiguriert, dass bei Eingabe einer unbekannten oder – wegen fehlender Anmeldung mit den Voucher-Daten – noch nicht zugänglichen Internetseite stets automatisch die Landing Page aufgerufen wird. Sie bietet dem Internet-Nutzer einen definierten Ansatzpunkt für die Benutzung des Hotspots.

Voucher: Gutschein, auf dem die Zugangsdaten aufgeführt sind, die dem Kunden die zeitlich limitierte Internet-Nutzung gestatten.

Das brauchen Sie

Um einen W-LAN-Hotspot zu betreiben, müssen verschiedene Voraussetzungen erfüllt sein:

Schneller Internet-Zugang (ADSL)

Access Point, Abrechnungsserver oder Vertrag mit einem Abrechnungsdienstleister

Falls erforderlich: Erlaubnis zur Installation der Antennen und Access Points (beim Vermieter oder Eigentümer des Grundstücks oder Ladenlokals einzuholen)

Berücksichtigung eventueller Denkmalschutzauflagen in alten Gebäuden

230-V-Stromversorgung an den Standorten der Geräte

Unter Umständen: Verlegung von Netzwerkkabeln nach CAT5

Ein kleiner Hotspot, der ein Ladenlokal oder Gasthaus versorgen soll, ist vergleichsweise einfach zu aufzubauen. Die größte Herausforderung ist die Wahl des besten Antennenstandorts, um eine optimale Ausleuchtung zu erreichen. Mit einfachen Tools, die mit einer W-LAN-Karte geliefert werden, können bereits gute Ergebnisse erzielt werden. Sollen größere Hotspots errichtet werden, empfiehlt sich ein professionelles Site Survey, um die besten Ergebnisse zu erreichen (lesen Sie dazu auch den Beitrag ab 96).

In der Regel werden die baulichen Anforderungen die größten Hürden darstellen, denn der Einrichtung des Hotspots soll schließlich keine aufwendige Renovierung vorausgehen. Meist dürfen keine Antennen im optisch sichtbaren Bereich erkennbar sein, um das Erscheinungsbild von Fassaden oder die vorhandenen Wanddekorationen nicht zu stören oder um Auflagen des Denkmalschutzes zu erfüllen. Damit ist die optimale Konzeption eines Hotspots möglicherweise eingeschränkt. Wenn Sie Access Points verwenden, die direkt über das Netzwerkkabel mit Strom versorgt werden, haben Sie die Anforderung der 230-V-Stromversorgung elegant erfüllt. Namhafte Hersteller bieten derartige Lösungen an. Die aufwendige und auffällige Installation einer Steckdose sowie die Verlegung eines zusätzlichen Starkstromkabels entfällt damit.

Fast eine Selbstverständlichkeit ist der schnelle Internet-Zugang via ADSL. Allerdings können beim Betrieb eines W-LAN-Hotspots die Kosten schnell explodieren, wenn Sie als Tarif für diesen Anschluss keine echte Flatrate wählen. Auch „Pseudo-Flatrates“, die eine Deckelung der Nutzung durch eine bestimmte Grenze im Datenvolumen vorsehen, sind nicht empfehlenswert, um einen Hotspot ins Internet zu bringen. Befindet sich der Hotspot nämlich in einem Café in der Nähe einer Fachhochschule oder Universität, dann kann sich die Kundschaft durchaus sehr intensiv und häufig im Internet bewegen. Bei der Auswahl des Tarifs sollten Sie auch beachten, dass verschiedene Provider bei bestimmten Tarifen den Betrieb eines Hotspots untersagen. Kritisch ist das Thema Breitbandzugang in ländlichen Gebieten, die nicht mit DSL versorgt werden können oder wo bestenfalls geringe Geschwindigkeiten möglich sind. Vorsichtig sollte ein potenzieller Hotspot-Betreiber auch bei satellitengestützten Internet-Zugängen sein, denn deren Nutzung ist häufig um ein vielfaches teurer als konventionelle Internet-Access-Lösungen.

Das entscheidende Hemmnis bei der Einrichtung eines Hotspots ist häufig das fehlende Know-how des Betreibers. Denn die Dienste eines Beraters sind oft sehr teuer und Individuallösungen zur Gestaltung des persönlichen Hotspots damit für einen kleinen Betreiber nicht rentabel. Hinzukommen die Folgekosten für die Wartung des Systems und die Software-Pflege. Daher bieten sich für Betreiber kleiner Hotspots die so genannten „Out-of-the-box“-Lösungen an. Eine solche Komplettlösung stellen wir in diesem Beitrag vor.

Worauf Sie bei der Konfiguration achten müssen

Eine Komplettlösung zur Einrichtung eines W-LAN-Hotspots nimmt dem Betreiber enorm viel administrativen Aufwand ab. Um vieles – vom Aufbau und der Grundkonfiguration des Servers über die Auswahl der passenden Geräte bis zu den elementaren Grundlagen eines professionellen Betriebssystems – muss sich der Betreiber nicht mehr kümmern. Dennoch ist es nicht damit getan, den Hotspot aus der Verpackung zu nehmen, aufzustellen, zu verkabeln und einzuschalten. Einige Konfigurationen muss jeder Hotspot-Betreiber in jedem Fall vornehmen, damit der Hotspot nicht manipuliert werden kann und Besucher sich nicht unbemerkt einen kostenlosen Internet-Zugang erschleichen können.

Sicherheit ist auch ein Thema, wenn es um den Schutz der Kunden geht. Man darf nicht voraussetzen, dass sie ihre Computer generell absichern oder sich der Bedeutung von „Freigaben“ der Ressourcen ihres Computers bewusst sind. An dieser Stelle muss der Betreiber aktiv werden und die Kommunikation von Computern innerhalb des Hotspot-Netzwerks verhindern (Intertraffic Blocking). Diese Funktion widerspricht zwar der klassischen Funktionsweise eines Netzwerks, ist jedoch bezeichnend für das Verantwortungsbewusstsein des Betreibers und damit für die Qualität seiner – mit dem Hotspot erbrachten – Dienstleistung.

COMPOINT: Access Points, die anstelle einer fest montierten Antenne den Anschluss einer externen Antenne zulassen, sind ideal für den Aufbau eines W-LAN-Hotspots.

Ein wichtiges Thema ist schließlich die Benutzerverwaltung. An dieser Stelle sollten Sie beachten, dass es der Hotspot-Betreiber ist, der aus Sicht seines Providers als Benutzer gilt. Es liegt also im Interesse des Hotspot-Betreibers, sicherzustellen, dass illegale Aktionen durch zwielichtige Kunden unterbunden werden. Es ist mittlerweile allgemein bekannt, dass sich der Traffic im Internet anhand der IP-Adresse bis zum Benutzer zurückverfolgen lässt. Der „Benutzer“ ist aber aus Sicht des Internet-Service-Providers nicht der anonyme Kunde im Hotspot-Bereich, sondern dessen Betreiber! Verbreitet ein Hotspot-Kunde über diesen Weg verbotenes Material im Internet, kann dies durchaus ernste Schwierigkeiten für den Hotspot-Betreiber bedeuten. Wer sich mit den Funktionen des Hotspots auskennt, wird in der Lage sein, im Zweifelsfall die „Notbremse“ zu ziehen und eine dubiose Sitzung zu beenden.

Einen kleinen Hotspot einrichten

Stellvertretend für eine Reihe ähnlicher Produktserien zeigen wir an dieser Stelle den Aufbau und die Administration eines W-LAN-Hotspots am Beispiel des Systems von Funkwerk En- →

PROFI-TIPP

Geld verdienen mit dem Hotspot

Wer eine Investition – beispielsweise in einen W-LAN-Hotspot – tätigt, fragt zuerst danach, wann sie sich wieder amortisieren wird. Bei einem W-LAN-Hotspot betrachtet man häufig nur die Erlöse aus dem Verkauf von Online-Zeiten. Das kann in vielen Fällen zu dem Ergebnis führen, dass der Hotspot vermeintlich unwirtschaftlich ist. Eine umfassende Betrachtung, die in erster Linie das Kerngeschäft im Auge hat, lässt die Situation aber in einem vollkommen anderen Licht erscheinen.

Konzeptbestandteil Der Hotspot ist dann plötzlich nicht mehr ein isoliertes Profitcenter, sondern Bestandteil des Gesamtkonzepts und aus dieser Sicht sehr lukrativ. Insbesondere im Gaststättengewerbe lassen sich interessante Ideen umsetzen. So könnte Online-Zeit als Rabatt auf den Verzehr angerechnet werden. Die Gäste kommen also nicht ausschließlich, um im Internet zu surfen, sondern nutzen die Möglichkeit, bei einem Kaffee persönliche E-Mails zu lesen. Was zunächst unterschiedslos erscheinen mag, differenziert sich in der Philosophie. Zunächst relativ geringem Internet-Umsatz stehen steigende Verzehrumsätze gegenüber. Idealerweise werden die Voucher mit einer befristeten Gültigkeitsdauer versehen, denn wer zum Surfen kommt, wird vermutlich auch wieder etwas konsumieren.

Werbeflächen verkaufen Ein weiterer Umsatzgenerator ist der Verkauf von Werbeflächen. Der Betreiber kann etwa einen kostenlos nutzbaren Bereich – den Walled Garden – definieren, in dem Webseiten zugänglich sind, die etwa Geschäfte in der Nachbarschaft bewerben.

terprise Communications (vormals: ARtem). Das System – eine klassische „Out-of-the-box"-Lösung – besteht im wesentlichen aus zwei Komponenten:

dem Common Public Access Server (ComPass) und
einem Access Point (ComPoint)

Während anstelle eines ComPoints auch nahezu jeder andere Access Point verwendet werden kann, ist der ComPass das Herzstück der Lösung. Er enthält – bereits weitgehend konfiguriert – alle wichtigen Funktionen des Hotspots. So übernimmt der ComPass das Anlegen der Benutzerkonten und das Verwalten der Guthabenkonten. Er ist gleichzeitig ein Webserver, auf dem die Startseite für den Kunden (Landing Page) und der Walled Garden verwaltet werden. Der ComPass stellt aber auch weitere grundlegende Server-Dienste zur Verfügung: Beim Zugriff auf das Internet arbeitet er wie ein Proxy-Server, der die Webseiten aus dem Internet holt und dem anfragenden PC zur Verfügung stellt. Noch bevor überhaupt eine produktive Kommunikation zwischen dem mobilen Computer und dem ComPass erfolgen kann, weist das Gerät dem neuen PC innerhalb des W-LAN in seiner Eigenschaft als DHCP-Server eine eigene IP-Adresse zu. Diese IP-Adresse ist allerdings lediglich in dem Netzabschnitt gültig, der durch den Funkbereich des Hotspots definiert ist. Weder in einem eventuell vorhandenen lokalen Netzwerk, in das der Hotspot für den Zugang zum Internet neben anderen Computern des Betreibers integriert ist, noch im Internet selbst ist diese IP-Adresse gültig.

Die Hardware installieren

Beim Aufstellen und der ersten Inbetriebnahme der Hardware sollten Sie unbedingt die Bedeutung der Anschlussbuchsen beachten. Bereits hier erfolgt die Trennung zwischen dem lokalen Bereich, also dem W-LAN, in dem die Kunden später auf den Server zugreifen werden, und dem WAN (Wide Area Network). An das WAN-Interface wird entweder ein DSL-Modem angeschlossen, das die Verbindung zum Internet herstellt, oder aber der ComPass in ein bestehendes lokales Netzwerk eingebunden, in dem es bereits – beispielsweise über einen Internet Access Router – eine Verbindung zum Internet gibt.

Der oder die Access Points – der im Beispiel verwendete ComPass bietet vier Schnittstellen, an die sich jeweils ein Access Point andocken lässt – werden an die vorgesehenen Buchsen angeschlossen. Wichtig ist bei dem gezeigten System allerdings, dass auch der Computer, mit dem die Konfiguration des Systems erfolgt, an einer solchen internen Schnittstelle betrieben wird. Darüber hinaus ist vor der Konfiguration die Einstellung der IP-Adresse im PC des Administrators zu beachten.

Für den Aufbau großflächiger W-LAN-Infrastrukturen, aber auch für Hotspots, sind Access Points ideal, die den Anschluss einer speziellen Antenne zulassen und nicht ausschließlich eine integrierte Antenne nutzen. Das ermöglicht es, über ein geeignetes Kabel die Antenne an einem günstigen Platz zu montieren, der eine optimale Ausleuchtung des zu versorgenden Bereichs gestattet. Unter Umständen – wenn nicht auch die Anzahl der gleichzeitig aktiven Benutzer eine dominante Rolle spielt – kann durch eine gute Wahl des Antennenstandorts ein Access Point bei der Versorgung großer Bereiche eingespart werden. Der Access Point lässt sich – aufgrund der räumlichen Trennung von der Antenne – an einem Ort installieren, an dem sowohl ein Netzwerkanschluss als auch eine 230-V-Energieversorgung vorhanden sind.

Erste Konfigurationsschritte

Beim ersten Einschalten des Systems wird schnell deutlich: In der kleinen blauen Kiste befindet sich ein vollwertiger PC. Zwar ist weder der Anschluss einer Maus noch der einer Tastatur vorgesehen und auch eine Monitorschnittstelle sucht man vergeblich, doch ist deutlich das Geräusch der integrierten Festplatte zu vernehmen. Der ComPass arbeitet mit dem Linux-Betriebssystem. Der Zugriff auf den Hotspot-Computer erfolgt über ein Web-Interface von einem PC des Administrators über einen der W-LAN-seitigen Ethernet-Ports.

Nach der ersten Anmeldung des Administrators am System mit den in der Dokumentation genannten Benutzerdaten ist zunächst einmal nur ein sehr karges Menü zugänglich, das lediglich gewisse Grundkonfigurationen, nicht aber das Anlegen und Verwalten von Benutzerkonten zulässt. Das hat seinen guten Grund, denn die Erfahrung zeigt, dass Default-Passwörter vom Anwender sehr häufig nicht geändert werden. Der Verzicht auf diese kleine Mühe kann jedoch sehr unangenehme Folgen haben, weil dann der Zugriff auf die Konfiguration jedem Angreifer mit etwas Fachwissen offensteht. Um dies zu ver-

PROFI-TIPP

Das richtige Tarifmodell wählen

Je nachdem, welches Hotspot-System zum Einsatz kommt oder welche Lizenzen der Betreiber erworben hat, stehen meist mehrere Alternativen zur Tarifgestaltung offen. Unabhängig vom Nutzungspreis ist der Ablauf der Online-Zeit ein wichtiges Kriterium.

Prepaid-Passed-Time Bei diesem Tarif läuft die Zeit nach dem ersten Login unwiederruflich ab. Dabei ist es gleichgültig, ob sich der Benutzer zwischenzeitlich ausloggt und eine Pause in der Nutzung einlegt.

Prepaid Used Time Anders sieht es dagegen beim Prepaid-Used-Time-Tarif aus. Hier reduziert sich das Guthaben des Benutzers nur dann, wenn er auch tatsächlich am Hotspot angemeldet ist. Diese Tarifform lässt es somit zu, das Guthaben über mehrere Sitzungen verteilt zu nutzen.

Prepaid-Passed-Time-Tarifmodelle eignen sich recht gut, wenn die Kunden einen „Rabatt" auf den Verzehr mit dem Hotspot-Voucher erhalten. Bezahlen die Kunden dagegen gezielt die Nutzung des Internet über den Hotspot, ist die Prepaid-Used-Time-Variante die fairste Lösung.

Testzugänge Der Betreiber kann auch Testzugänge und Gruppentarife definieren, die außerhalb der regulären Tarife die Nutzung ermöglichen. Mit einem Testzugang kann der Kunde etwa nach der Eröffnung des Hotspots die Möglichkeit bekommen, sich ein Bild von den Leistungsmerkmalen zu machen. Die Kunden können aber auch – zunächst ohne finanziellen Aufwand – den Umgang mit dem Hotspot erlernen.

Gruppentarife Sie bieten sich an, wenn beispielsweise Räume für eine Sitzung vermietet werden und in dieser Zeit auch die Nutzung des Internets über den Hotspot kostenlos enthalten sein soll. Das Anlegen und Ausgeben von individuellen Vouchern wäre in diesem Fall viel zu aufwendig.

DER EXPERTEN-TIPP

Hotspots benutzerfreundlich einrichten

Die modernen Geschäftsnomaden, aber auch technik-affine Privatnutzer suchen zunehmend drahtlose Breitband-Internet-Anschlüsse – W-LAN-Hotspots –, um eine neue Art der Mobilität auszuleben. Diese Hotspots werden meist von mobilen Carriern oder Wireless-Internet-Service-Providern (WISP) betrieben. Die Qualität des Services ist dabei höchst unterschiedlich und nicht immer zur Zufriedenheit der Benutzer. Wo liegen also die Tücken?

Der Benutzerkomfort sollte möglichst hoch sein. Falsche Notebook-Konfigurationen, etwa feste IP-Adresse, Proxy-Einstellungen oder E-Mail-Einstellungen, beim Benutzer sollte das System tolerant handhaben. Denn ist der Kunde gezwungen, erst die Netzwerkeinstellungen zu konfigurieren, führt die damit verbundene Fehlerträchtigkeit oft zur Unzufriedenheit der Benutzer.

Intelligente Gateways, etwa von Nomadix, die auch bei großen Business-Hotspots wie der Messe Frankfurt, Messe Hannover oder in großen Hotels eingesetzt werden, sorgen für konfigurationsfreien Nutzerkomfort. Die meisten großen Anbieter sparen aber gerade bei kleinen Hotspots an entsprechender Hardware und verärgern damit ihre Kunden nachhaltig.

Für Hotspot-Betreiber gibt es deshalb die Möglichkeit, ihren Internet-Service maßgeschneidert ihren Kunden anzubieten und entsprechend selbst zu verdienen. Ein Beispiel dafür ist das ASP-Angebot von mobileLounge (www.mobileLounge.net). Bei diesem ASP-Modell kann der Hotspot-Betreiber selbst entscheiden, welches Angebot für den Kunden gratis ist, ab wann das Internet-Angebot kostenpflichtig wird und wie die Portalseite des Standorts aussieht.

Individuelles Angebot So schafft der Betreiber ein attraktives Portal, bei dem wichtige Informationsquellen, etwa das Angebot von Fluggesellschaften, Flughäfen oder Bahn, sowie sonstige News-Dienste, etwa Tageszeitungen, Börseninformationen oder regionale Städteportale, kostenlos angeboten werden können. Damit lässt sich die Attraktivität des Hotspot-Standorts beträchtlich erhöhen.

CHIP EXPERTE

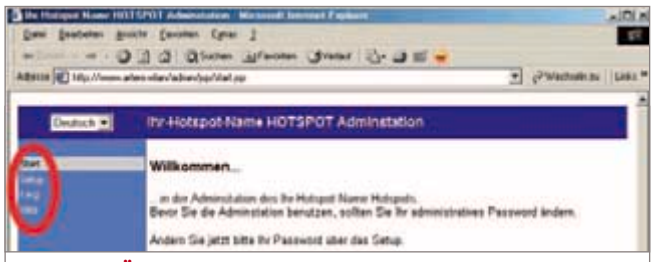
Hans Franzl ist Geschäftsführer der brainworks computer technologie GmbH in Feldkirchen. Das Unternehmen wurde 1989 gegründet und beschäftigt sich mit der Distribution von Netzwerk- und Systemmanagement-Produkten mit den zugehörigen Dienstleistungen.

→ www.brainworks.de

meiden, blockiert der ComPass alle wichtigen Funktionen so lange, bis der Administrator ein neues Zugangspasswort gewählt hat. Ein individuelles Kennwort lässt sich im Setup-Menü festlegen, das in dieser Phase als einziges Menü mit direkten Konfigurationsmöglichkeiten nutzbar ist.

Über das Setup-Menü ist auch eine für den allgemeinen Betrieb des Hotspots sehr wichtige Konfiguration zugänglich: die Definition des Internet-Zugangs.

Je nachdem, wie der Zugang zum Internet erfolgt, muss der erste Konfigurationsschritt so aussehen: Bei einem direkten Zugang per DSL werden die Daten benötigt, die der Internet-Service-Provider zur Verfügung gestellt hat. Das sind mindestens der Benutzername und das Passwort. In diesem Beispiel wird der ComPass in ein lokales Netzwerk integriert, in dem sich ein Internet-Access-Router befindet. Das LAN kann mit einer festen IP-Adressenstruktur arbeiten, was die Administration für den Laien jedoch sehr kompliziert macht. Häufig werden die IP-Adressen aber automatisch von einem DHCP-Server vergeben. Ein solcher DHCP-Server ist meist Bestandteil eines guten Internet-Access-Routers. In diesem Fall muss für den Zugang zum Internet lediglich „LAN“ ausgewählt und die Einstellung auf „DHCP“ vorgenommen werden.



EINGESCHRÄNKT: Solange der Administrator nicht sein eigenes Zugangskennwort geändert hat, stehen aus Sicherheitsgründen nur sehr wenige Menüpunkte zur Auswahl.

In den Public-Access-Parametern werden die Stationskennung und der Name des Hotspots definiert. Die Stationskennung ist stets Bestandteil der Benutzernamen, die das System automatisch generiert. Damit ist eine eindeutige Zuordnung der Voucher zum jeweiligen Hotspot möglich. In diesem Menü lässt sich auch die Homepage des Betreibers eintragen. Die steht dann als direkter Link im Hauptmenü der Landing Page zur Verfügung und kann auch von den Benutzern erreicht werden, die keinen Voucher erworben haben.

Der Walled Garden ist ein offener Bereich des Hotspots. Dort können Internet-Adressen eingetragen werden, die kostenlos erreichbar sein sollen. In Frage kommen etwa weitere Internet-Adressen des Betreibers oder Internet-Adressen von Werbepartnern, die für die Erreichbarkeit im Walled Garden des Hotspots bezahlen. Das in unserem Beispiel gezeigte kleine Kompaktsystem lässt die Definition von acht frei erreichbaren Internet-Adressen zu. Zu beachten ist allerdings, dass über diese Adressen aufgerufene Links nicht kostenlos erreichbar sind. Eine Suchanfrage über eine im Walled Garden eingetragene Suchmaschine wird zwar eine Ergebnisliste liefern, allerdings wird keines der darin angegebenen Ziele ohne vorherige Anmeldung mit gültigen Benutzerdaten aufrufbar sein.

Sehr wichtig und ebenfalls bereits in der Erstkonfiguration festzulegen ist der IP-Adressbereich für die PCs der Kunden, die im Hotspot auf das Internet zugreifen wollen. Im W-LAN-Bereich arbeitet der ComPass generell als DHCP-Server. Das ist die Voraussetzung dafür, dass fremde Computer ohne administrativen Aufwand die Landing Page des Hotspots aufrufen können. Sobald ein PC in den Sendebereich des Hotspots gelangt und dessen Konfiguration – keine Definition einer bestimmten SSID, keine aktivierte Verschlüsselung und kein automatischer Bezug der IP-Adresse aus dem Netzwerk – es zulässt, bekommt dieser Rechner vom ComPass eine IP-Adresse sowie die entsprechenden Daten für das Standard-Gateway und den →

DNS automatisch zugewiesen. Sowohl der Adressbereich, aus dem die Adresse vergeben wird, als auch die Dauer der Zuweisung einer Adresse (Lease Time) wird vom Betreiber des Hotspots vorgegeben. Für die Festlegung des Adressbereichs müssen drei Felder beachtet werden: Die W-LAN-Basisadresse entspricht der Netzwerk-Adresse. Es werden nur die Dezimalzahlen – durch jeweils einen Punkt voneinander getrennt – eingegeben, die den Teil der IP-Adresse beschreiben, der in anderen Systemen von der Netzmaske beschrieben wird. Die Felder „DHCP-Start“ und „DHCP-Ende“ bezeichnen die Computer-Adressen (Host-Adressen) innerhalb dieses Netzes.

Ein Beispiel: Die Netzwerkadresse 192.168.2.0 mit einer Netzmaske von 255.255.255.0 (klassische Darstellung einer Klasse-C-IP-Adresse) wird als W-LAN-Basisadresse folgendermaßen dargestellt: 192.168.2

Die Start- und End-Adressen ergänzen die fehlende Stelle, wobei jedoch die Adressen 0 (kennzeichnet die Netzwerk-Adresse) und 255 (Broadcasting) nicht vergeben werden dürfen. Im Beispiel scheiden darüber hinaus die Hostadressen 1 und 2 ebenfalls aus, weil diese dem ComPass und dem Access Point fest zugewiesen sind.

Neben der Definition des Passworts gehört dieses Menü nicht nur zu den wichtigsten, sondern auch zu den kritischsten Menüs in der Grundkonfiguration. Die Veränderung des W-LAN-Domainnamen muss in jedem Fall für künftige Zugriffe auf die Administrationsoberfläche beachtet werden. Wer an dieser Stelle eine eigene Domain kreiert, muss diese anstelle der in der Schnellstart-Anleitung vermerkten W-LAN-Domain verwenden. Mit den bisher genutzten Daten kann die Konfiguration nicht mehr erreicht werden.

Schließlich wird in diesem Menü festgelegt, wie sicher sich der Kunde fühlen kann, wenn er seine Benutzerdaten zur Anmeldung in die Landing Page einträgt. Generell sollte das HTTPS-Protokoll gewählt werden Dadurch werden die Benutzerdaten zwischen dem Computer des Kunden und dem ComPass über einen SSL-gesicherten Kanal übertragen. Das Mithören der Zugangsdaten und deren Missbrauch durch Dritte ist damit weitgehend ausgeschlossen.

Die Landing Page gestalten

„Out of the box“-Lösungen erfordern stets Kompromisse zwischen einer einfachen Einrichtung beziehungsweise Benutzerführung des Administrators und den Gestaltungsmöglichkeiten des Systems. Besonders deutlich wird dies bei der Landing Page, die nur mit wenigen grafischen Elementen in einem vorgegebenen Rohdesign gestaltet werden kann. Sie können zunächst einmal ein Logo setzen, das auf allen vom ComPass gehosteten Seiten stets an der gleichen Stelle erscheint und eine klare optische Referenz zum Betreiber darstellt (Corporate Identity). Darüber hinaus lässt sich eine Blickfanggrafik auf der Landing Page plazieren, wobei es jedoch gewisse Einschränkungen gibt. So müssen alle Grafiken mit einem festen Seitenverhältnis angelegt werden, da die Bilder sonst verzerrt dargestellt werden. Auch ist es nicht möglich, Hotspots – hier im Sinne des Web-Designs verstanden – zu setzen, die verschiedene Darstellungen der Grafik mit jeweils individuell passenden Hyperlinks verbinden. Ebenso muss der Betreiber bei den Texten Abstriche machen, denn es lassen sich ausschließlich ein Info- und ein AGB-Text nach den eigenen Vorstellungen gestalten – mit der Einschränkung, dass keine weiteren Hyperlinks gesetzt werden können. Die Texte müssen Sie als einfache, unformatierte Textdateien anlegen.

Was aus der Sicht eines Profis im Web-Design wie ein gravierender Nachteil des Systems aussieht, hat durchaus seinen Sinn: „Out-of-the-box“-Lösungen sollen den Betreiber nicht technisch überfordern, denn man geht davon aus, dass es eben keine IT-Profis sind, die sich für diese Systeme entscheiden. Nur mit den gegebenen Einschränkungen ist also gewährleistet, dass die Funktionen der Landing Page, also die Anmeldeprozedur und die Links des Walled Garden, auch tatsächlich in der gewünschten Form funktionieren.

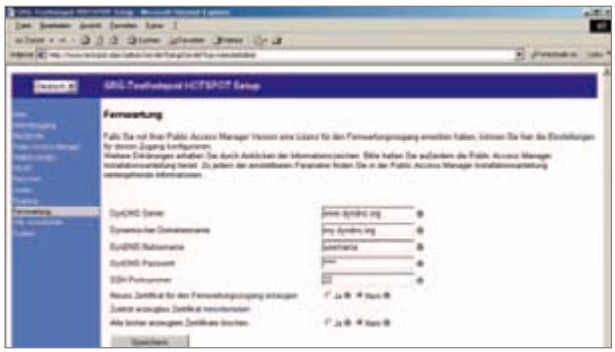
Benutzerverwaltung organisieren

Der Hotspot hat nun bereits ein für den Betrieb des Systems geeignetes Erscheinungsbild. Die Koordination der IP-Adressen ist erledigt und der Administratorbereich des ComPass ist mit einem neuen Kennwort vor Missbrauch geschützt. Was noch fehlt, sind die Kunden. Diese haben möglicherweise ihr Notebook bereits aufgeklappt und möchten auf das Internet zugreifen. Die Landing Page und auch die im Walled Garden freigegebenen Seiten sind schon erreichbar. Um aber alle Adressen im Internet ansteuern zu können, benötigen die Kunden individuelle Account-Daten, die der ComPass generiert. In anderen Systemen ist es auch möglich, die Zugangsdaten vom Server eines Abrechnungsdienstleisters abzurufen.

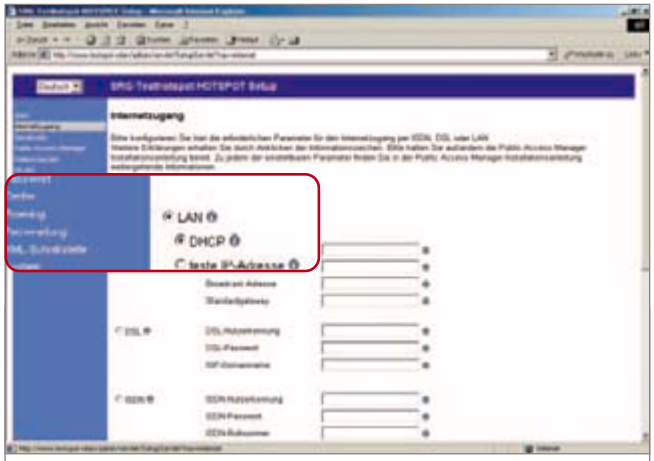
PROFI-TIPP

Fernwartung ermöglichen

Der in diesem Beitrag beschriebene Hotspot erlaubt auch die Fernwartung über das Internet. Sichere Fernwartung Damit dies in einer gesicherten Form erfolgen kann, werden Zertifikate verwendet, die zuvor vom ComPass angelegt wurden. Der Betreiber muss dieses Zertifikat vom Server laden und auf seinem PC speichern. Damit kann im Problemfall ein Administrator direkten Zugang zum Hotspot bekommen und dem Betreiber ohne Wegezeiten kostengünstigen Support leisten.



NOTHILFE: Zielgruppe einer kompakten Hotspot-Lösung sind nicht unbedingt absolute T-Experten. Daher ist eine sichere Möglichkeit zur Fernwartung durch einen kompetenten Administrator sehr wichtig.



COMPASS KONFIGURIEREN: Ein DHCP-Server vergibt die IP-Adressen im Netz automatisch, was viel Handarbeit erspart. Aktivieren Sie daher die Optionen „LAN“ und „DHCP“.

Sollen die Benutzerkonten von ComPass angelegt werden, absolviert der Administrator die folgenden Schritte:

Zuerst einmal muss er festlegen, welchem Tarif die zu erstellenden Voucher zugehören. Dabei können verschiedene Online-Zeiten gewählt werden. Darüber hinaus kann er – eine entsprechende Lizenz vorausgesetzt – bestimmen, ob der Voucher unabhängig von der tatsächlichen Nutzung nach dem ersten Login abläuft (Prepaid Passed Time) oder ob der Kunde sein Guthaben über verschiedene Sitzungen hinweg nutzen kann (Prepaid Used Time).

Nachdem die Voucher-Daten im System angelegt sind, muss der Administrator sie herunterladen. Er kann die Daten als Textdokument in tabellarischer Form speichern und weiterverarbeiten. Aufgrund der Struktur des Textes ist es möglich, die Daten nach einer Konvertierung in eine Tabellenkalkulation oder in eine Datenbank zu übernehmen. Aus diesen Applikationen können nun einzelne Datensätze ausgewählt und auf Gutscheinen gedruckt werden. Bevor dies jedoch möglich ist, muss der Administrator den Erhalt der Voucher-Daten noch quittieren. Erst jetzt sind die Benutzerkonten im System gültig und lassen sich von den Kunden zur Anmeldung am Hotspot nutzen. Erwähnenswert sind noch zwei weitere Tarifformen, die sich mit dem gezeigten Hotspot realisieren lassen – der freie Zugang und der Gruppenzugang (siehe auch Kasten 104).

Freien Kunden-Zugang einrichten

Besonders in der Einführungszeit des Hotspots kann es sich langfristig lohnen, den potenziellen Kunden eine kostenlose Testmöglichkeit anzubieten. Allerdings soll sich auch in dieser Zeit das System bereits refinanzieren. Aus diesem Grunde ist eine zeitliche Begrenzung des kostenlosen „Schnupperzugangs“ sinnvoll. Weil auch an dieser Stelle eine einfache Handhabung des Systems im Vordergrund steht, ist der freie Zugang bereits vorkonfiguriert worden. Der Betreiber des Hotspots muss lediglich noch einstellen, ob und wie lange den Kunden ein freier Zugang gewährt werden soll. Zur Wahl stehen dabei Zeiten von zehn und 30 Minuten.

Ist der freie Zugang aktiviert, taucht auf der Landing Page ein entsprechender Link auf. Der Benutzer gelangt über diesen Link auf eine vom ComPass angelegte Webseite, in der er seine E-Mail-Adresse eintragen muss. Dieser Schritt reduziert die Wahrscheinlichkeit einer mehrfachen Nutzung des freien Zugangs durch einen einzigen Benutzer, sodass sich das finanzielle Risiko für den Betreiber in Grenzen hält. Nach der Eingabe der E-Mail-Adresse bekommt der Benutzer seine Zugangsdaten angezeigt, die er notieren und später in den Login-Dialog des Hotspots eingeben muss. Die Zugangsdaten haben das gleiche Format wie die eines gekauften Vouchers. Der Benutzer kann also nicht nur die Funktion des Hotspots als solche testen, sondern hat auch die Möglichkeit, sich ohne jedes eigene finanzielle Risiko an den Umgang mit diesem öffentlichen Internet-Zugang zu gewöhnen.

Gruppenzugang einrichten

Betreiber von Hotels und Gaststätten bieten ihren Gästen in der Regel auch die Nutzung ihrer Räumlichkeiten für Seminare oder Tagungen an. Dieser Service wird mit der Verfügbarkeit eines drahtlosen Internet-Zugangs noch attraktiver. Allerdings dauern Tagungen in der Regel einige Stunden und es ist allgemein unklar, wie viele der Teilnehmer den Zugang zum Internet benötigen. Theoretisch ist es denkbar, jedem Teilnehmer pauschal einen Voucher mit einem limitierten Zeitkonto zur Verfügung zu stellen, doch ist dies ein großer administrativer Aufwand für den Betreiber des Hotspots. Darüber hinaus wird es einzelne Teilnehmer der Sitzung geben, denen die zur Verfügung gestellte Online-Zeit nicht ausreichen wird. Andere wiederum nutzen nur wenige Minuten des Guthabens oder verzichten ganz darauf. Möglicherweise werden die Voucher dann bei anderen Gelegenheiten von den Teilnehmern privat verwendet. In jedem Fall ist es sehr aufwendig und uneffektiv, mit klassischen Vouchern einer ganzen Gruppe für einen begrenzten Zeitraum einen möglichst ungehinderten Zugriff auf das Internet zu ermöglichen.

Eine gute Alternative ist das Freischalten eines Gruppenzugangs. Der Betreiber des Hotspots definiert dabei lediglich einen einzigen Account – bestehend aus einer Benutzerkennung und einem Passwort – und teilt diese Daten den Sitzungsteilnehmern mit. Mit diesen Kennungen können sich nun die Miglieder in nahezu beliebiger Anzahl über die gesamte Dauer der Tagung frei im Internet bewegen. Die Anzahl der Sitzungsteilnehmer, die gleichzeitig auf das Internet zugreifen können, ist lediglich durch das Limit des Hotspots als solches begrenzt. In diesem Beispiel – es kommt ein ComPass XT-20 zum Einsatz – können über den Hotspot bis zu 20 Benutzer gleichzeitig auf das Internet zugreifen. Diese Zahl ist sinnvoll, weil bei höheren Benutzerzahlen keine zufriedenstellende Performance mehr gewährleistet werden kann; auch die Leistungsgrenzen des verwendeten Internet-Zugangs spielen bei dieser Frage eine wichtige Rolle.

Der Vorteil eines zentralen Gruppenzugangs besteht neben dem Komfort für den Kunden, der sich ungestört durch administrative Zwänge (Nachkauf von Vouchern etc.) voll auf seine Tagung konzentrieren kann, auch in der erheblich vereinfachten Verwaltung dieses Accounts durch den Betreiber des Hotspots. Obwohl der Account mit der Einrichtung für 24 Stunden aktiviert wird, hat der Betreiber stets die volle Hoheit über sein →

System, denn der Gruppenzugang lässt sich mit einem Mausklick deaktivieren, sobald die Tagung beendet ist.

Den ersten Kunden versorgen

Jetzt ist es soweit: Der Hotspot ist konfiguriert, und die Benutzerkonten sind angelegt. Die vom Server des Hotspots generierten beziehungsweise vom Abrechnungsdienstleister gelieferten Zugangsdaten liegen in Form gedruckter Vouchers vor und können verkauft werden. Der erste Kunde sitzt schon mit seinem Notebook am Tisch und möchte sein persönliches E-Mail-Postfach im Internet öffnen. Seine erste Hürde besteht nun darin, die Startseite – die Landing Page – des Hotspots zu finden. Damit dies klappt, muss das Notebook des Kunden einige Voraussetzungen erfüllen:

Der Computer muss so konfiguriert sein, dass er seine IP-Adresse von einem DHCP-Server automatisch beziehen kann.

Die W-LAN-Karte muss mit einem neutralen Profil betrieben werden. Es sollte also keine SSID beziehungsweise kein Netzwerkname vorgegeben sein. Alle Verschlüsselungsfunktionen müssen deaktiviert sein.

Sehr zu empfehlen: Alle Freigaben von Ressourcen des Notebooks (Zugriff auf Dateien oder Verzeichnisse beziehungsweise einen angeschlossenen Drucker) sollten deaktiviert sein. An dieser Stelle steht die Sicherheit des Kunden im Vordergrund, denn man kann sich nie darauf verlassen, ob der Betreiber des Hotspots tatsächlich den Traffic innerhalb des W-LAN-Bereichs blockiert hat.

Wer vertrauliche Daten übertragen möchte, sollte beachten, dass er sich im Internet und damit in einem ungeschützten Netzwerk befindet. Angemessene Sicherheitsmaßnahmen, beispielsweise ein gesichertes VPN, sind also zu empfehlen.

Einige ältere oder mit Applikationen aus OpenSource-Quellen zusammengesetzte Hotspot-Lösungen sehen meist kein automatisches Routing auf die Landing Page vor. Der Kunde muss in diesem Fall die Adresse der Landing Page, die auf den Voucher aufgedruckt ist, exakt in die Adressleiste des Browsers eingeben. Dies führt oft zu kontroversen Diskussionen zwischen dem Hotspot-Betreiber und seinen Kunden.

Gute Lösungen – auch bei Kompaktsystemen darf man das erwarten – bieten dem Kunden weit mehr Komfort und arbeiten mit einem integrierten Domain Name Server. Anhand von dessen Einträgen und dem Vergleich mit den Berechtigungen des Kunden wird geprüft, ob die vom Kunden eingegebene Adresse im kostenlosen Bereich jedermann zugänglich ist oder im Internet liegt. Ist der Benutzer mit einem gültigen Account am System angemeldet, wird die Anfrage an das Internet weitergegeben. Andernfalls sendet der ComPass seine Landing Page an den Benutzer. Beim vorgestellten System ist es also vollkommen gleichgültig, welche Adresse der Benutzer in die Adressleiste einträgt. Solange er nicht am System angemeldet ist, bekommt er – abgesehen von den Adressen im Walled Garden – grundsätzlich die Landing Page zu Gesicht.

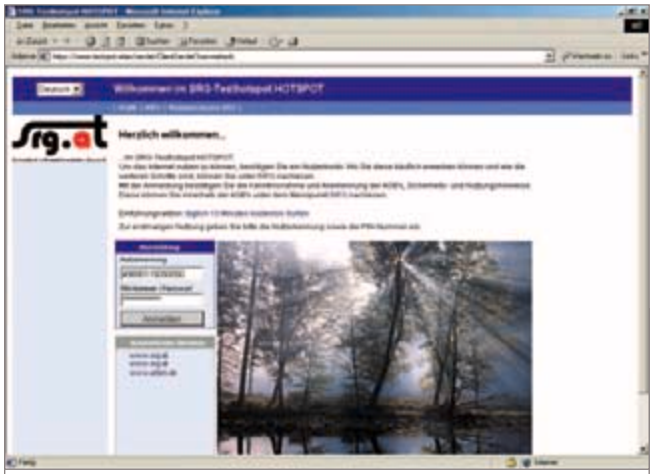
Dort findet der Kunde den Anmeldedialog, in dem er den Benutzernamen und sein Kennwort – beides ist auf dem Voucher vermerkt – eintragen kann. Der Kunde sollte stets das Browser-Fenster mit der Landing Page geöffnet halten und weitere Aktivitäten in einem neuen Fenster starten. Auf diese Weise behält er am einfachsten die Übersicht über sein Restguthaben und kann sich jederzeit bequem vom Hotspot abmelden, was insbesondere bei einem Prepaid-Used-Time-Tarif, der zum mehrmaligen Einloggen berechtigt, sinnvoll ist.

So behalten Sie den Überblick

„Der Kunde ist König", heißt es, doch ändert dies nichts daran, dass der Betreiber des Hotspots niemals den Überblick über die Vorgänge in seinem System verlieren darf. Ein Blick auf das Display seines Access-Servers verrät ihm bereits, ob eine Verbindung mit dem Internet besteht und wie viele Benutzer gerade im Hotspot aktiv sind. Nähere Informationen bekommt der Betreiber über seinen Administratoren-Account direkt vom Server. So kann er beispielsweise feststellen, wie viele Benutzerkonten noch verfügbar sind. Dabei handelt es sich um die Konten, die zwar angelegt, aber noch nie am System angemeldet wurden. Doch an dieser Stellle ist Vorsicht geboten, denn eine Aussage darüber, wie viele Voucher tatsächlich bereits verkauft wurden, kann diese Statistik nicht bieten!

Die Übersicht zu den aktiven Benutzerkonten verrät, wie viele Voucher mindestens einmal im System angemeldet waren und deren Guthaben noch nicht aufgebraucht ist. Diese Information kann auch den aktuellen Status (gerade online oder offline) angeben, allerdings ist es bei einem größeren Kundenkreis nicht erforderlich, die augenblicklich im System angemeldeten Kunden zu listen. Dafür gibt es eine eigene Funktion im Menü, mit der die tatsächlich gerade im System angemeldeten Benutzer gelistet werden können.

Übersichten allein sind jedoch noch kein effektives administratives Werkzeug. Für den Betreiber des Hotspots ist es wichtig, bei Bedarf einzelne Kunden gezielt sperren oder ihnen auch Hilfestellung geben zu können. So kann der Benutzer durchaus das vom ComPass generierte Passwort ändern und ein eigenes Zugangskennwort festlegen. Das ist sogar zu empfehlen und sollte als Hinweis auf den Voucher aufgedruckt werden. Vergisst der Kunde jedoch sein neues Passwort, hat auch der Administrator keine Chance, es aus dem Server auszulesen und dem Kunden mitzuteilen. Allerdings kann der Betreiber des Hotspots



STARTSEITE: Die Landing Page des Hotspots sieht zwei Eingabefelder für die Nutzerkennung und das Passwort vor. Diese Daten sind auf dem Voucher des Kunden aufgedruckt.

die Zugangsdaten in den ursprünglichen Zustand, so wie sie auf dem Voucher aufgedruckt sind, zurücksetzen, und der Kunde kann seinen Account weiternutzen.

W-LAN-Hotspot absichern

Sicherheit im Wireless LAN ist ein brisantes Thema: Es wird beispielsweise über wirksame Verschlüsselungsverfahren diskutiert, um ein Abhören des Netzwerk-Traffics, einen Missbrauch der Ressourcen und des Internet-Zugangs zu vermeiden. Sicherheit ist auch bei einem W-LAN-Hotspot ein wichtiges Thema, allerdings gelten an dieser Stelle völlig andere Voraussetzungen als in einem privaten Netz. So ist der Hotspot ein öffentlich zugängliches System, das keinesfalls – beispielsweise durch Unterdrücken der SSID – „versteckt" werden soll. Unrealistisch ist es darüber hinaus, die Übertragung auf der Funkschnittstelle zu verschlüsseln. Dies würde voraussetzen, dass jedem Benutzer der Schlüssel bekannt ist. Der Schlüssel wäre dann allgemein bekannt und die Sicherheitsmaßnahme damit unwirksam. Abgesehen davon reduziert jeder noch so geringe Aufwand für den Kunden die Akzeptanz des Hotspots. Der will nämlich sofort und ohne weitere Konfigurationen seiner Netzwerkeigenschaften über den Hotspot online gehen.

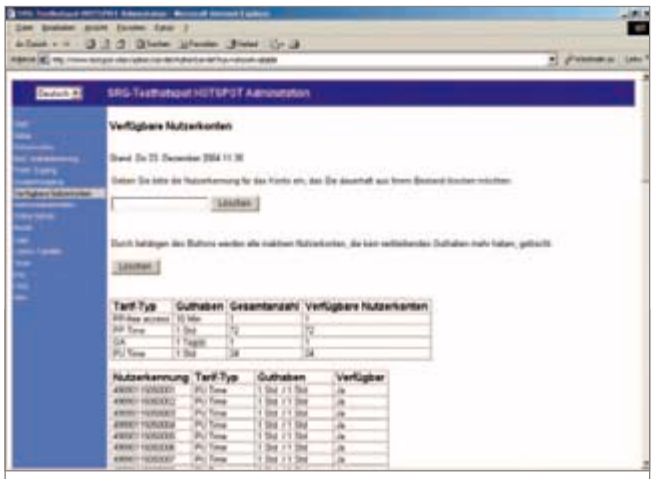
Dennoch hat der Betreiber verschiedene Möglichkeiten, um seinem Kunden ein weitgehend sicheres Agieren im Hotspot zu erlauben. Das beginnt mit einer Beratung zu den gegebenen Sicherheitsgrenzen und setzt sich über aktive Sicherheitsmaßnahmen am System fort.

Abhörschutz beim Login aktivieren

Die reine Datenkommunikation zwischen dem Notebook des Kunden und dem Hotspot lässt sich mit aktuellen Verfahren noch nicht absichern. Zwar könnte man sich durchaus Lösungen vorstellen, doch stehen die dafür anfallenden Kosten in keinem Verhältnis zu Aufwand und Nutzen.

Anders sieht es dagegen bei der Anmeldung des Benutzers am Hotspot aus. Einige Systeme – so auch der in diesem Beispiel gezeigte Hotspot – bieten die Möglichkeit, die Anmeldung über eine SSL-Verschlüsselung abzusichern. Das Aktivieren dieser Sicherheitsfunktion ist in unserer Beispielkonfiguration etwas versteckt im W-LAN-Menü vorzunehmen. An dieser Stelle wird in der letzten Zeile das Portal-Protokoll ausgewählt. Nur bei der Wahl von HTTPS erfolgt später eine gesicherte Anmeldung am Hotspot. Diese Einstellung ist in jedem Fall zu empfehlen, zumal alle modernen Browser die SSL-Verschlüsselung unterstützen.

Allerdings ist dabei lediglich der Anmeldedialog, nicht aber die eigentliche Datentransaktion gesichert.



ALLE KUNDEN IM BLICK: Der Administrator-Account liefert dem Hotspot-Betreiber zahlreiche Übersichten, beispielsweise wie viele Kunden mit welchem Guthaben gerade aktiv sind.

Intertraffic Blocking einrichten

Ein großes Sicherheitsproblem im W-LAN-Hotspot sind die Freigaben von Ressourcen auf den PCs der Kunden. Während diese ihre W-LAN-Karte im Büro oder daheim zur Vernetzung mit bekannten Rechnern nutzen und innerhalb dieses Netzwerks möglicherweise Speicherplatz auf der eigenen Festplatte zur Verfügung stellen, ist der Zugriff Unbekannter innerhalb des Sendebereichs im Hotspot unerwünscht. Sowohl der Kunde als auch der Betreiber des Hotspots können dagegen etwas tun: Der Kunde sollte darauf achten, dass Freigaben generell deaktiviert sind, sobald er sich in einem ungesicherten Netzwerk aufhält. Das macht etwas Mühe, verhindert aber den Zugriff von Angreifern auf den eigenen PC am wirksamsten. Der Betreiber des Hotspots kann Hacker mit Hilfe des so genannten Intertraffic Blocking abwehren.

Intertraffic Blocking wird nicht am ComPass aktiviert, sondern erfordert einen direkten Eingriff in die Konfiguration des Access Points. Dort gibt es je nach Modell und Hersteller verschiedene Möglichkeiten. Ein weiteres Problem, das insbesondere dem technischen Laien erhebliche Schwierigkeiten bereiten kann, besteht darin, dass Intertraffic Blocking als solches in der Regel nicht in den Menüs zu finden ist.

Im Falle eines Funkwerk-Access-Points wie in unserem Beispiel-Hotspot muss die Konfiguration des W-LAN-Ports (w11_ap) aufgerufen und die Funktion „Repeating" deaktiviert werden. Auf diese Weise wird die Kommunikation zweier Computer innerhalb des W-LAN unterbunden. Ein Hacker am Nebentisch kann also nicht mehr innerhalb des Hotspots auf die Festplatte seines Tischnachbarn zugreifen. Auch Portscans sind ausgeschlossen, ebenso wie der Zugriff auf einen benachbarten PC über das Internet, denn lediglich der ComPass verfügt über eine im Internet gültige IP-Adresse. Die vom ComPass im W-LAN-Bereich den Kunden-Computern zugewiesenen IP-Adressen sind im Internet weder bekannt noch direkt zugänglich.

Allerdings hat dieses Verfahren zur Vermeidung internen Traffics im Hotspot auch einen Nachteil, denn es bezieht sich ausschließlich auf die Funkschnittstelle eines einzigen Access Points. Flächenmäßig größere Hotspots erfordern jedoch zwei oder mehr Access Points. Wird ausschließlich die Repeating-Funktion deaktiviert, ist immer noch ein Angriff über einen zweiten Access Point möglich. Der Angreifer muss also lediglich den Platz wechseln, um zum Erfolg zu kommen. Das ist inakzeptabel und so müssen weitere Sperren in den Access Points konfiguriert werden. Am wirksamsten ist es, wenn die Kommunikation mit anderen Access Points durch das Setzen von Filtern unterbunden wird.

Robert Schoblick

Wireless Bridges

W-LAN statt Festnetz

Das Verlegen von Netzwerkkabeln ist aufwendig, teuer und verlangt beim Überschreiten von Grundstücksgrenzen beinahe schon juristisches Fachwissen. Für Distanzen von bis zu fünf Kilometer Luftlinie – bei direkter Sichtverbindung – bietet die W-LAN-Technologie jedoch eine gute Alternative zum Kabel.

Man stelle sich folgendes Beispiel vor: In zwei Gebäuden, zwischen denen eine öffentliche Straße verläuft, befinden sich die Büros einer Firma. Denkbar ist auch, dass sich in einem Gebäude ein Geschäft und in dem anderen die Privatwohnung des Geschäftsinhabers befindet. Nun soll zwischen den beiden Standorten eine Netzwerk- und möglicherweise auch eine Telefonverbindung hergestellt werden. Technisch ist das keine Herausforderung – allerdings stellt die zwischen den Gebäuden liegende Straße ein Problem dar, das die direkte Verlegung eines Kabels unmöglich macht. Bereits bei diesem einfachen Szenario müssten also Festverbindungen eines öffentlichen Netzbetreibers angemietet werden, die sehr teuer sind. Eine gute Alternative ist eine Richtfunkstrecke, die preiswert und auch mit wenig technischem Aufwand zu realisieren ist.

Wann eine Wireless Bridge möglich ist

Der Aufbau einer solchen Wireless Bridge ist jedoch nur unter bestimmten Voraussetzungen möglich:

Die Distanz der zu verbindenden Standorte darf nicht größer als fünf Kilometer sein, wobei dieser Wert unter Experten als sehr optimistisch angenommen wird (siehe Kasten auf 111).

Zwischen den Antennen beider Standorte muss eine direkte optische Sichtverbindung bestehen. Weder Bauwerke noch Kräne oder Bäume dürfen also die Sicht auf die gegenüberliegende Antenne versperren.

Technisch wird die Wireless Bridge aus zwei W-LAN-Access Points realisiert, die in einem speziellen Bridge-Modus betrieben werden können. Das ist wichtig, weil bereits der physikalische Zugriff der Geräte auf die Funkschnittstelle davon ausgeht, dass nur eine einzige Gegenstelle existiert (bei Point-to-Point-Bridge). Da eine Wireless Bridge in der Regel Entfernungen überwindet, die im klassischen Infrastruktur-Modus (W-LAN-Client-Karten kommunizieren mit dem Access Point) nicht erreichbar sind, wird in den meisten Fällen an den beiden Standorten jeweils eine spezielle Antenne mit Richtcharakteristik benötigt. Eine solche Richtantenne bündelt ihre Sendeleistung beziehungsweise -empfindlichkeit in eine Richtung, wodurch sie die Signalenergie optimal aufnehmen und abstrahlen kann. In den anderen Richtungen sind die Wirkungen einer Richtantenne deshalb minimal.

Outdoor-Antennen richtig einsetzen

Um eine Wireless Bridge mit größerer Reichweite (mehr als 500 Meter) zu errichten, empfiehlt sich generell der Einsatz von Outdoor-Antennen. Die müssen mit geeigneten Kabeln an den Access Point angeschlossen werden. Ganz wichtig ist, dass die verschiedenen Hersteller meist eigene Anschlusssysteme für die Antenne vorsehen. Ideal sind Schraubverbindungen, die einen stabilen Halt des Steckers gewährleisten und damit Störungen reduzieren. Allerdings gibt es keine einheitliche, herstellerübergreifende Vereinbarung zur Wahl des Steckersystems, sodass Sie in der Regel Access Points, Kabel und Antennen vom gleichen Anbieter beziehen sollten.

Bei Outdoor-Antennen sollte Sie außerdem beachten, dass diese im Jahresverlauf extremen Klimaschwankungen ausgesetzt sind. Schon bei der Montage ist deshalb zu berücksichtigen, dass ein einzelner Mast bereits eine erhebliche Windlast darstellen kann. Darüber hinaus sind die Bestimmungen der jeweils geltenden Blitzschutzvorschriften (etwa DIN V VDE 0185 Teil 100) zu berücksichtigen, die den Einsatz von Blitz- und Überspannungsableitern sowie von Erdungsmaßnahmen regeln.

CHIP → DVD-CODE W-LAN

- → **Optimiert** WLAN Expert zeigt die Signalstärke von WLAN-Netzen an. Der Antennen-Test ermittelt die Qualität des Funksignals und erleichtert die Wahl des besten Standorts.
- → **Sicheres Netz** Schützen Sie Ihr WLAN, indem Sie potenziellen Angreifern mit dem Tool FakeAP tausende weitere Access Points in der Nähe vorgaukeln.

PROFI-TIPP

W-LAN-Bridge anmelden

Auch wenn sie die Grundstücksgrenzen in ihrer Funktion überschreitet, muss eine Wireless Bridge nicht genehmigt werden. Der Betrieb der W-LAN-Karten und Access Points nach IEEE 802.11 a/b/g ist mit einer allgemeinen Genehmigung zugelassen. Allerdings ist der Betrieb einer Wireless Bridge meldepflichtig, wenn sie grundstücksüberschreitend betrieben wird.

Schriftlich melden Mitteilungsformulare, mit denen der Betreiber der Wireless Bridge seiner Meldepflicht nachkommen kann, werden in der Regel von den Herstellern der Geräte zur Verfügung gestellt. Sie können ein solches Formular beispielsweise auch vom Webserver von Funkwerk Enterprise Communications als Datei im PDF-Format herunterladen (www.artem.de/content/artem/artem000275/Bridge_Meldeformular.pdf.

Formulare bestellen Die Amtsblätter können Sie auch bei der Regulierungsbehörde für Telekommunikation und Post bestellen. Weitere Bezugsmöglichkeiten für die Formulare sind im Internet unter www.regtp.de abrufbar.

Die besten Wireless-Bridge-Tipps im Web

W-LAN-Bridge in der Praxis → www.wlan-skynet.de/docs/richtfunk/wlan-vergleich.shtml
Hintergrundinformationen zu Wireless Bridges
Wireless Bridge richtig installieren → www.artem.de/content/artem/artem000173/ar_ig_BridgeLinks_d.pdf
Sehr anschaulicher Installationsleitfaden von Artem
Vorbereitungen → www.oe1.oevsv.at/funkfeld.htm
Wichtige Informationen zur Funkfeldplanung

Unabhängig davon empfiehlt sich zum Schutz der angeschlossenen Geräte ein Überspannungsschutzmodul.

Eine Wireless Bridge einrichten

Die Konfiguration der Access Points – die Endpunkte einer Wireless Bridge – ist wenig spektakulär. Nur einige wichtige Details sind zu beachten, die sowohl die Funktion als auch die Sicherheit der Wireless Bridge gewährleisten. So beginnt die Konfiguration jedes Access Points – egal, in welchem Betriebsmodus er arbeiten soll – mit der Zuweisung eines neuen Netzwerknamens, des Service Set Identifier (SSID). Der dient der eindeutigen Abgrenzung der übertragenen Daten von Systemen, die in unmittelbarer Nachbarschaft möglicherweise auf der gleichen Frequenz funken. Aus Sicherheitsgründen schalten Sie den SSID-Broadcast aus. Diese Maßnahme macht die SSID auf der Funkschnittstelle – entgegen verbreiteten Ansichten – nicht generell unsichtbar, denn sie kann bei detaillierter Netzwerkanalyse von einem W-LAN-Experten nach wie vor gefunden werden. Sie erhöht jedoch den Aufwand für Angreifer enorm. Auch die Zuweisung der IP-Adressen gehört zur Standardkonfiguration eines jeden Access Point. Die IPs können sowohl automatisch von einem DHCP-Server als auch manuell vom Administrator fest vergeben werden. Auf der LAN-Seite des Access Points erleichtert die Kenntnis einer festen IP-Adresse dem Administrator den Zugriff auf das Gerät.

UNBEDINGT VERSCHLÜSSELN: Auch für eine Wireless Bridge sollten Sie eine möglichst starke Verschlüsselung aktivieren – etwa mit einer Tiefe von 152 Bit wie in der Abbildung.

KNOW-HOW

Die Grenzen von W-LAN-Bridges

In der Fachliteratur spricht man von Reichweiten von bis zu fünf Kilometern für eine Wireless Bridge. Die sind unter wirklich guten Bedingungen auch realistisch, doch müssen auch Kompromisse akzeptiert werden. Eine der wichtigsten Einschränkungen ist zweifellos die Geschwindigkeit. W-LAN-Bridges, die auf die maximale Reichweite eingerichtet sind, arbeiten nämlich sehr langsam.

Tempo-Einbußen Trotz guter Antennen und Access Points sind bei Distanzen im Kilometerbereich in der Regel nur maximal 1 bis 2 MBit/s – gemeint sind natürlich die Burstgeschwindigkeiten der W-LAN-Systeme, keinesfalls die messbare Netto-Transferrate – erreicht. Weitere Probleme können auftreten, wenn eine Wireless Bridge bei gutem Wetter im Grenzbereich ihrer Möglichkeiten eingerichtet wird und auch zu funktionieren scheint. Denn bei den ersten Niederschlägen – ob Nebel, Regen oder Schnee – kann die Funkstrecke plötzlich zusammenbrechen. Der Grund besteht in den dämpfenden Eigenschaften des Wassers für Mikrowellen.

Auf Reserven achten Die Wassertropfen in der Luft absorbieren die Energie des W-LAN-Signals sehr stark. Ein gutes Design einer Wireless Bridge wird deshalb niemals ohne Reserven auskommen. Auch bei der Wahl der Antenne empfiehlt es sich, auf einen hohen Gewinn und eine gute Richtcharakteristik zu achten. Dies gewährleistet zwar unter schwierigen klimatischen Bedingungen bei großen Distanzen nicht die maximale Performance, bietet aber gute Chancen, dass die Strecke tatsächlich funktionsfähig bleibt.

Die eigentliche Konfiguration des Access Points als eine Seite einer Wireless Bridge erfolgt durch die Festlegung des Betriebsmodus. Der Access Point kann etwa als Point-to-Point-Bridge, als Point-to-Multipoint-Bridge, als klassischer Access Point in einer W-LAN-Infrastruktur, als Repeater oder als W-LAN-Client (einer W-LAN-Netzwerkkarte vergleichbar) eingesetzt werden. Wählen Sie den Betriebsmodus einer Wireless Bridge, werden die Gegenstellen anhand ihrer MAC-Adresse definiert. Diese Vorgabe ermöglicht es dem Gerät, sein Pendant über die Entfernung zu identifizieren und eine Verbindung herzustellen. Darüber hinaus ist mit der Definition der MAC-Adresse auch eine zusätzliche Sicherheitsbarriere geschaffen, die ein potenzieller Angreifer zunächst einmal überwinden muss.

Die Wireless Bridge ist ein über mehrere hundert Meter – unter Umständen sogar mehrere Kilometer – reichendes Kommunikationsmedium, über das auch sensible Daten laufen können. Verzichten Sie allerdings auf eine Verschlüsselung, wird Angreifern damit möglicherweise eine Hintertür in das lokale Netzwerk mit uneingeschränktem Zugriff auf Server und andere Systemressourcen geöffnet.

Das Aktivieren der Verschlüsselungsfunktionen, die mittlerweile jedes W-LAN-Produkt mitbringt, sollte deshalb auch beim Aufbau einer Wireless Bridge obligatorisch sein. Das gilt auch dann, wenn ausschließlich die Minimalverschlüsselung mit 64 Bit verfügbar ist. Für eine Wireless Bridge empfiehlt es sich allerdings, eine möglichst große Schlüsselbreite zu verwenden. In Netzen, in denen Sicherheit eine besonders große Bedeutung →

DER EXPERTEN-TIPP

Ideal zum Vernetzen von Großveranstaltungen

Die wohl herausragendsten Eigenschaften einer Wireless Bridge auf der Basis konventioneller W-LAN-Technologie sind ihre Flexibilität, die einfache Installation und die geringen Kosten der Systemkomponenten.

Zeitlich begrenzter Einsatz Damit sind Wireless Bridges ideal in temporären Infrastrukturen einsetzbar, etwa zur Versorgung der Organisatoren von Sportveranstaltungen mit einer Netzwerkinfrastruktur. Die Arbeitsplätze der Administration und für Korrespondenten können so in kurzer Zeit vernetzt werden. An diesen Arbeitsplätzen sorgen entweder drahtgebundene Hubs oder Switches oder wiederum W-LAN-Systeme für den Anschluss der einzelnen Computer. Trotz des vergleichsweise einfachen Aufbaus sind Wireless Bridges aber nur eingeschränkt als Plug & Play-Lösung zu betrachten. Dichte Vegetation bei Outdoor-Systemen stört die Funksignale und erfordert nicht selten den Einsatz einer „Relaisstation", um einen Umweg zu realisieren, oder aber eines konventionellen Netzes.

Bridges im Dauereinsatz Auch für dauerhafte Verbindungen lassen sich Wireless Bridges ohne weiteres einsetzen. Allerdings sollte die Entfernung zwischen den vernetzten Bereichen nicht allzu groß sein, damit eine möglichst hohe Übertragungsgeschwindigkeit erreicht werden kann. Selbst innerhalb von Gebäuden sind Wireless Bridges sinnvoll nutzbar, etwa zum Vernetzen von W-LAN-Access-Points zur Erweiterung drahtloser Infrastrukturen ohne zusätzlichen Verkabelungsaufwand.

Flexible Ergänzung Wireless Bridges ersetzen also keinesfalls etablierte Systeme wie Festverbindungen, optischen Richtfunk und dergleichen, doch können sie durchaus eine wirtschaftliche und technische Lücke bei der Planung großflächiger Netzwerke schließen. Zudem prädestiniert sie der rasche Aufbau für kurzfristige Einsätze.

CHIP EXPERTE

Bernhard Knaus ist selbständiger EDV-Berater und Web-Designer in Pörtschach am Wörthersee (Österreich).

→ www.knabe.at

spielt, sollte der Administrator darüber hinaus durch den zusätzlichen Einsatz eines IPSec-VPN (Virtuel Private Network) eine starke Verschlüsselung anbieten und damit auch die Integrität sowie die Authentizität der beteiligten Gegenstellen des Netzwerks gewährleisten.

Die Antennen richtig montieren

Insbesondere im Outdoor-Bereich werden an die Antennen hohe Anforderungen gestellt, die nicht allein der Funktion, sondern auch der Sicherheit von System und Gebäude dienen. Das wichtigste Element eines solchen Antennensystems ist deshalb die Erdung: Sowohl der Mast als auch ein in die Antennenleitung zu integrierender Überspannungsschutz sind mit einem geeignet großen Querschnitt zu erden. Empfohlen wird beispielsweise die Erdung mitels eines Kupferleiters mit einem Querschnitt von 16 Quadratmillimetern. Wichtig: Der Überspannungsableiter in der Antennenleitung ersetzt kein Blitzschutzsystem des Gebäudes, bestehend aus Fangeinrichtung, Ableiter und Erdung (mit geringem Erdübergangswiderstand) sowie ein abgestuftes Überstrom-/Überspannungsableitersystem in den elektrischen Anlagen.

Bei der Montage der Antenne ist zudem zu beachten, dass diese eine gewisse Windlast aufweist. Die Antenne muss also auch stürmischem Wetter standhalten können. Dazu sollten Sie einen geeigneten Mast und dem Mauerwerk entsprechendes Befestigungsmaterial wählen. Das gilt insbesondere dann, wenn die Antenne an einem langen Mast sehr hoch über das Hausdach ragen muss (wichtig auch wegen des erhöhten Risikos von Blitzeinschlägen).

Natürlich soll eine Wireless Bridge möglichst gute Übertragungseigenschaften aufweisen. Das erreichen Sie durch eine geringe Dämpfung des gesamten Hochfrequenzbereichs – ausgehend vom Access Point bis zum Eingang des Access Points auf der Gegenseite.

Einen dämpfenden Einfluss haben auch die Antennenleitungen und die Verbindungsstellen. Ideal ist es deshalb, wenn die Antennenleitung zwischen dem Access Point und der Antenne möglichst kurz gewählt wird. Es ist deshalb besser, den Access Point in unmittelbarer Nähe zur Antenne zu installieren und diesen unter Umständen mit einem Power-over-Ethernet-Konzept mit Betriebsstrom zu versorgen, anstatt lange Koaxialkabel zu verlegen. Verbesserungen der Übertragungseigenschaften erreicht man auch in der Wahl von Antennen mit einem hohen Gewinn und durch den Einsatz von Empfangsverstärkern.

Robert Schoblick

KNOW-HOW

Voice over IP via Wireless Bridge

Wer den Aufbau einer Wireless Bridge in Erwägung zieht, möchte oft sowohl zeitunkritische Computerdaten als auch Sprache in Echtzeit übertragen. Das ist prinzipiell möglich, denn im Gegensatz zu einer W-LAN-Infrastruktur kommuniziert eine Wireless Bridge (Point to Point) nur mit einer einzigen Gegenstelle. Den beiden Gegenstellen steht damit die volle Kapazität der Übertragungsstrecke zur Verfügung.

Leistungseinbußen Allerdings kann eine Wireless Bridge in der Performance durchaus von benachbarten Netzen beeinträchtigt werden, wenn diese auf dem gleichen Kanal arbeiten. Soll die Funkstrecke sowohl Daten als auch Voice-over-IP-Pakete oder sogar Videosequenzen übertragen, sollten Sie einkalkulieren, dass Sie dabei auf ein wesentlich langsameres Medium umsteigen.

Bandbreiten managen Notwendig sind also vor den Access Points der Wireless Bridge Maßnahmen für das Bandbreitenmanagement, um den VoIP-Paketen eine Priorität bei der Belegung der Funkstrecke oder eine garantierte Mindestbandbreite zuzuweisen. Grundsätzlich aber ist Voice over IP über eine Wireless Bridge sehr wohl möglich und letztlich auch eine attraktive Alternative zu den klassischen Leitungswegen des öffentlichen Telefonnetzes.

Vermaschte Funknetze

Mesh-Netze mit W-LAN

Topologien auf der Grundlage von Wireless LAN bieten vielfältige und flexible Möglichkeiten der Vernetzung. Die Anwendungen reichen von Heimnetzen, bei denen Access Points gleichzeitig Zugangs- und Relaispunkt sind, bis hin zu W-LAN-basierender öffentlicher Infrastruktur, etwa alternative Stadtnetze. CHIP zeigt die Hintergründe.

Mit der zunehmenden Verbreitung drahtloser Netze gerät eine weitere Forschungsdisziplin immer mehr in den Fokus von Produktentwicklung und Produktimplementierung: Multi-Hop- und vollvermaschte Topologien. Im einfachsten Fall können W-LAN-Stationen zusätzlich zu ihrer eigentlichen Funktion eine Routing-Funktion übernehmen. Insbesondere kann ein Access Point sowohl Bridge sein – und damit die Verbindung zu einem anderen W-LAN-Subnetz herstellen – als auch als Zugangspunkt aktiv werden (lesen Sie zu W-LAN-Bridges den Beitrag ab 110). Wird dieser Gedanke weiterentwickelt, können unter Verwendung mehrerer Stationen leistungsfähige, flexible und vor allem selbstorganisierende adaptive Infrastrukturen aufgebaut werden. In diesem Beitrag werden die wichtigsten theoretischen Grundlagen diskutiert und einige wichtige praktische Implementierungen dieser so genannten Mobile Ad-Hoc Networks (MANET) vorgestellt. Dieser Beitrag konzentriert sich auf Techniken, Geräte und Installationen, die auf IEEE802.11 (W-LANs) basieren.

GLOSSAR

Adaptives Netzwerk Funktionalität eines Netzwerks, auf veränderte Situationen – etwa Lastveränderungen, ausgefallene oder nicht erreichbare Stationen – zu reagieren und eine aktuelle, optimierte Topologie zu gewährleisten.

Ad-Hoc-Netzwerk Funktionalität eines Netzwerks, das eine automatische Verwaltung der beteiligten Stationen und insbesondere deren An- und Abmeldung erlaubt.

Mesh-Netzwerk Netzwerk-Topologie, bei der Stationen nicht nur mit einem zentralen Knoten, sondern mit vielen benachbarten Stationen unmittelbar kommunizieren können.

Multi-Hop-Netzwerk Netzwerk-Topologie, bei der Funkstationen über Relaisstationen erreicht werden. Multi-Hop-Netzwerke weisen im Gegensatz zu Mesh-Netzwerken meist eine hierarchische Struktur auf.

Wireless ISP Internet-Service-Provider, der sich auf die Bereitstellung von drahtlosen Zugangsnetzen (WLAAN) konzentriert.

WLAAN Wireless Local Area Access Network, das den Zugang zu einer übergeordneten Netzebene, z.B. Internet, mit WLAN- Technologien erreicht.

Ausgangssituation bei drahtgebundenen Netzen

Bei drahtgebundenen Netzwerken herrschen im Bereich der lokalen Netze (LANs) heute im allgemeinen Bus-, Stern- oder Baum-Topologien vor, da bei ihnen der Verdrahtungsaufwand und die Anzahl der verfügbaren Netzwerkschnittstellen in einem sinnvollen Verhältnis stehen. Allerdings weisen diese Topologien die folgenden Einschränkungen auf.

Zuverlässigkeit: Sie besitzen eine Bisektionsbreite von 1. Das bedeutet, dass beim Ausfall einer Verbindung die Kommunikation unterbrochen ist.

Adaptivität und Lastverteilung (Load Sharing): Bei Ethernet werden beispielsweise mit Hilfe des Spanning-Tree-Protokolls (STP) redundante Verbindungen komplett abgeschaltet, um den gefürchteten Broadcast-Sturm zu vermeiden.

Lediglich im Bereich des Grid-Computing werden Rechner in meist zweidimensionalen Arrays miteinander verschaltet, um eine engere Kopplung und eine Abbildung des meist matrizenorientierten Datenstroms auf die Topologie zu erreichen. Aber bereits bei einem 2D-Gitter werden pro Rechner vier Netzwerkkarten und ein entsprechender Verdrahtungsaufwand benötigt.

Im Bereich der Weitverkehrsnetze (WAN) findet man Ringe und teilvermaschte Topologien. Bei diesen Topologien rechtfertigen die Verfügbarkeitsanforderungen die höheren Kosten. Die Bisektionsbreite beträgt mindestens 2.

Drahtlose Netze

In den meisten bestehenden W-LAN-Architekturen wird es als einer der größten Nachteile angesehen, dass die Stationen auf ein Shared Medium zugreifen und sich die verfügbare Bandbreite teilen müssen. Ebenso wird die inhärent begrenzte Reichweite oft als Nachteil empfunden.

Beide vermeintlichen Nachteile stellen aber die Grundlage für die sehr viel höhere Flexibilität bei der Festlegung von Netztopologien dar. Insbesondere lassen sich auch mit einer Funkschnittstelle pro Station vermaschte Topologien realisieren. Im einfachsten Fall kommuniziert jeder Knoten mit seinen jeweiligen Nachbarn, sodass sich recht unmittelbar ein 2D-Gitter ergibt, wie es in der Info-Grafik auf 116 oben links zu sehen ist. Bei einer sehr engen räumlichen Anordnung kann sich auch eine vollvermaschte Topologie ergeben (siehe Info-Grafik auf 116 oben rechts), bei der jede Station mit jeder anderen unmittelbar kommunizieren kann.

Mit solchen vermaschten Topologien können die folgenden Vorteile erreicht werden:

Jeder Knoten übernimmt die Funktion sowohl eines Endknotens, der Verkehr generiert oder konsumiert, als auch die Funktion eines Zwischenknotens, der den Datenverkehr weiterleitet. Es werden somit keine dezidierten Geräte, beispielsweise Bridges oder Router, als Zwischenknoten benötigt. Im allgemeinsten Fall handelt es sich bei dieser Topologie um besondere Peer-to-Peer-Architekturen, da nicht nur alle Knoten Dienste anbieten und konsumieren, sondern auch Verkehr weiterleiten können.

Die besten Mesh-Tipps im Web

Nichtkommerzielle Netze → www.freifunk.net/
Deutsche Webseite für freie (Funk-)Netze und W-LAN mit Hintergründen über und Einsichten in die Community
Access Point für Mesh-Netze → http://meshcube.org/
Produkt-Infos zum Meshcube mit Link zur Wiki-Seite
Alternative Stadt-Netze → www.cuwireless.net/
Zahlreiche Informationen über „community-owned, not-for-profit broadband networks in cities and towns around the globe"

Zwischen unterschiedlichen Knoten existieren zahlreiche verschiedene Wege, sodass sowohl ein Load Sharing als auch eine extrem hohe Ausfallsicherheit gewährleistet werden können.
Ein weiterer Vorteil gerade bei drahtlosen Netzen besteht darin, dass mobile Stationen auch außerhalb des eigentlichen Empfangsbereichs einer Basisstation erreicht werden können, wenn andere Stationen als Repeater funktionieren. Solche Kettenverbindungen bezeichnet man auch als Multi-Hop-Netzwerke.

Herausforderungen bei drahtlosen Netzen

Bei vermaschten Funknetzen sind jedoch auch einige Nachteile und zusätzliche Herausforderungen zu berücksichtigen:
Wenn alle Stationen auch die Aufgaben von Zwischenknoten erfüllen, müssen sie über die entsprechende Funktionalität verfügen. Sie müssen also ständig eingeschaltet sein und werden zusätzlich belastet.
Wenn Endstationen auch Zwischenstationen sind, transportieren sie auch nicht an sie gerichteten Verkehr, wodurch sich eine zusätzliche Sicherheitsproblematik ergibt.
An die Routing-Algorithmen werden erhöhte Anforderungen gestellt, da in besonderem Maße auf Schleifenfreiheit geachtet werden muss. Ein wesentlicher Parameter dabei ist der Grad der Mobilität der vermaschten Stationen.
Um eine möglichst flexible Struktur zu erreichen, werden die Funkstationen oft auf den gleichen Kanälen betrieben. Dadurch verschärft sich die Problematik des Shared Medium, da immer nur eine Station pro Bereich senden kann. Zusätzlich sind die Problemfelder der versteckten Stationen (so genannte Hidden Stations) und der sichtbaren Stationen (Exposed Stations) zu berücksichtigen, für die herkömmliche Kanalzugriffsmechanismen (Medium Access Control, MAC) nur ansatzweise Lösungen erlauben.

Insbesondere die ersten beiden Aspekte dieses Abschnitts lassen sich durch einen zweistufigen Aufbau ausgleichen, indem nur Zwischenstationen miteinander verbunden werden. Die Endstationen werden über herkömmliche Sterntopologien an diesen Zwischenstationen betrieben, sodass sich die in der Grafik auf 116 gezeigten Topologien ergeben. Dies bringt übrigens zusätzlich eine Komplexitätsreduzierung der Routingalgorithmen mit sich, da sich die Topologie der vermaschten Stationen in der Regel nur noch langsam ändert, während die Mobilität der Endstationen auf normales Roaming begrenzt werden kann.

Routing-Algorithmen

Dynamische Routing-Algorithmen stellen die wesentliche Grundlage dar, auf der sich Mobile Ad-Hoc-Netzwerke selbst organisieren können. Die damit verbundenen Ideen wurden schon in den sechziger Jahren von Paul Baran beschrieben; sie sind die Grundlagen für die dynamischen Routing-Protokolle des Internets (mehr Informationen dazu finden Sie unter **www.rand.org/publications/RM/baran.list.html**).

Die für drahtlose vermaschte Netze entwickelten Algorithmen müssen den besonderen Anforderungen eng gekoppelter, dynamischer und störungsbehafteter Topologien Rechnung tragen. Dabei unterscheidet man zwei grundsätzliche Ansätze:
1. Bei tabellenbasierenden oder Distanzvektor-Protokollen wird der proaktive Versuch unternommen, die Route von einem Knoten zu jedem anderen Knoten im Netzwerk zu speichern. Bei komplexen Topologien steigt der Aufwand sehr stark, sodass sich in diesem Bereich auch hierarchische Ansätze gebildet haben. Vorteilhaft ist, dass die Tabellen teilweise auch statisch vorgegeben werden können. Zu den für die Praxis relevantesten Vertretern zählen
das Destination-Sequenced Distance-Vector (DSDV)-Routingprotokoll und
das Hazy Sighted Link State (HSLS)-Routingprotokoll.
2. Bei der zweiten Gruppe geht die Aktivität bedarfsorientiert vom Quellknoten aus (Source-Oriented On-Demand Driven). Dieser Ansatz verspricht eine sehr viel größere Flexibilität, bringt aber in der Regel schlechteres Echtzeitverhalten mit sich. Die bekanntesten Realisierungen in dieser Familie sind:
das dynamische Source Routing (DSR)-Routingprotokoll (mehr Informationen dazu finden Sie unter **www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt**) sowie
das Ad Hoc On Demand Distance Vector (AODV)-Routingprotokoll, das als RFC 3561 beschrieben ist (mehr Informationen bietet die Website **www.ietf.org/rfc/rfc3561.txt**) und als Linux-Kernel-Modul unter anderem von NIST zur Verfügung steht (mehr Informationen dazu finden Sie unter **http://w3.antd.nist.gov/wctg/aodv_kernel/**).

Systembeispiele

Community-Netze: Im Bereich der drahtlosen lokalen Netze (W-LAN) existieren mannigfache Ansätze zur Realisierung vermaschter Netze. Im Zentrum des Interesses stehen seit geraumer Zeit die so genannten Community-Netze oder Wireless Local Area Access Networks (WLAAN), bei denen eine W-LAN-basierende Infrastruktur ganze Stadtteile abdeckt und so eine alternative Struktur zu kommerziellen Internet-Service-Providern (ISPs) schafft. Dafür gibt es mittlerweile viele Beispiele, die sehr oft aus der Open-Source-Community stammen.
Hardware-Plattformen: Für die Realisierung der Hardware-Plattformen hat sich mittlerweile bei allen Unterschieden im Detail ein gemeinsames Architekturkonzept durchgesetzt.

Für die Funkanbindung kommen kommerziell erhältliche (Commercially Available Off-the-Shelf, COTS) W-LAN-Chipsets zum Einsatz.

Als Prozessor-Plattform werden meist kleinere 32-Bit-Prozessoren eingesetzt, wobei sich insbesondere die Intel-Architektur IA-32 oder ARM-Controller bewährt haben. Die Prozessoren müssen über eine adäquate Rechenleistung verfügen und eine moderate Verlustleistung erlauben, sodass das Gerät mit geringer Stromaufnahme rund um die Uhr ohne weitere Belästi- →

gung (etwa Lüftergeräusche), betrieben werden kann. Die meisten Plattformen setzen auf einem (Embedded) Linux auf. Dies hat den Vorteil, dass weitere Bestandteile, beispielsweise Treiber, aber auch Security-Implementierungen, problemlos übernommen werden können.

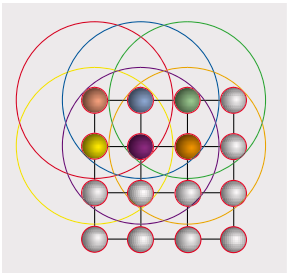
KNOW-HOW

Flache Topologien für Mesh-Netze

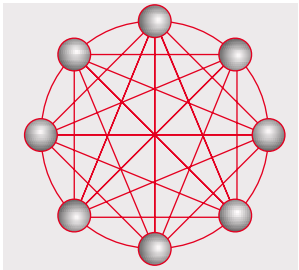
Bei flachen Topologien hat jede Station die gleiche Funktionalität in Bezug auf die Verbindung im Netzwerk. Drahtlose Netze ermöglichen an dieser Stelle eine große Flexibilität. 2-D-Gitter ergeben sich durch die beschränkte Reichweite der Funkstationen. Im unten gezeigten Beispiel kann jede Station direkt mit jedem unmittelbaren Nachbarn kommunizieren.

Voll vermaschte Topologien ergeben sich, wenn alle Stationen in einem gemeinsamen Empfangsbereich liegen.

Beide Topologien haben sich bei drahtgebundenen Netzen aufgrund der immensen Kosten nur in Spezialfällen etablieren können.



2D-Gitter



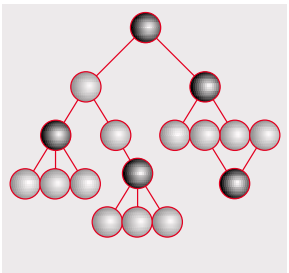
Voll vermaschte Topologie

Hierarchische Topologien

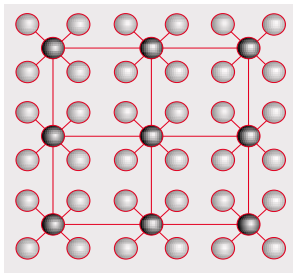
Hierarchische Topologien implizieren unterschiedliche Klassen von Geräten.

Der Cluster-Baum ist auch von drahtgebundenen Netzwerken im Sinne einer strukturierten Verkabelung bekannt. Auf den höheren Ebenen treten Bündelverkehr und höhere Geschwindigkeitsstufen auf. Bei drahtlosen Netzwerken ergibt sich die Hierarchie durch gestufte Funktionalität oder durch höhere Geschwindigkeiten. Ein Beispiel ist die auf dem erheblich schnelleren WiMAX-Standard basierende Kopplung von lokalen IEEE802.11-WLAN-Access Points.

Auch ein 2D-Gitter mit lokalen Sterntopologien lässt sich mit diesem gestuften Aufbau realisieren.



Cluster-Baum (übergeordnete Stationen in Schwarz)



Hierarchisches 2D-Gitter mit lokaler Sterntopologie

Quelle: Prof. Dr. Axel Sikora; Illustration: CHIP S. Schönberger

Neben vielen anderen Ansätzen ist in Deutschland in besonderem Maße auf die Linux-basierende OpenSource-Distribution MeshCube hinzuweisen (mehr Informationen dazu finden Sie unter **http://meshcube.org**), die wesentlich von dem Hamburger Unternehmen 4g-Systems entwickelt wurde (weiterführende Informationen unter **http://4g-systems.biz**). Es gibt aber auch zahlreiche generische Ansätze, beispielsweise OpenAP (mehr Informationen dazu finden Sie unter **http://opensource.instant802.com/hardware.php**).

Installationen: Auf diesen Hardware-Plattformen werden die Routing-Protokolle implementiert und in zahlreichen Installationen aufgebaut. Im Zusammenhang mit diesen Installationen bilden sich Erfahrungen und gute Praktiken heraus, die wieder zurückwirken auf die Entwicklung von Routing-Algorithmen und Geräten. Die meisten dieser Installationen entstehen ohne jeglichen kommerziellen Hintergrund, zumal ansonsten – zumindest in Deutschland – einer Carrier-Lizenz der Regulierungsbehörde für Telekommunikation und Post (RegTP) notwendig werden würde.

Die vermutlich bekannteste Installation beschäftigt sich sehr stark mit den algorithmischen Grundlagen. Das Roofnet-Projekt des Massachusetts Institute of Technology (MIT) wird im Bostoner Stadtteil Cambridge mit derzeit 92 Access Points betrieben (mehr Informationen dazu finden Sie unter **www.pdos.lcs.mit.edu/ roofnet/**). Es verwendet den SrcCC-Routing-Algorithmus.

Das Champaign-Urbana Community Wireless Network (CUWiN) entstand im Umfeld der Universität von Urbana (weitere Informationen unter **www.cuwireless. net/**). Es setzt auf einem adaptierten HSLS-Protokoll auf.

In Europa ist die Installation des Wireless Community Networks im niederländischen Leiden auf Grund des hohen Anteils von Eigenentwicklungen hervorzuheben (mehr Informationen dazu finden Sie unter **www.wirelessleiden.nl**).

Auch in Deutschland gibt es zahlreiche Beispiele, die Sie im Internet unter der Adresse **www.freifunk.net** aufgeführt finden.

Die Zukunft der Mesh-Netze

Mesh-Netzwerke auf W-LAN-Basis finden immer mehr praktische Anwendung. Auch wenn die diesbezüglichen Entwicklungen weder den Hardware-Herstellern noch den Internet-Service-Providern gelegen kommen, wurde 2004 die Arbeitsgruppe IEEE802.11s „ESS Mesh Networking“ ins Leben gerufen, die die zahlreichen verschiedenen Aktivitäten herstellerübergreifend standardisieren soll.

Es lässt sich also vermuten, dass wir – nach etwa 30 Jahren Forschung – immer noch am Anfang der Entwicklung stehen. Neben den W-LAN-basierenden Systemen, die auch auf absehbare Zeit mit Hardware- und Installationskosten von einigen wenigen hundert Euro pro Station zu Buche schlagen, werden in erheblichem Maße auch kostengünstigere Sensor-Aktor-Netzwerke nach dem ZigBee-Standard entwickelt, die in der Regel über sehr viel einfachere Funkschnittstellen, kleinere Prozessoren und günstigere Antennen verfügen – zu erheblich niedrigeren Preisen von einigen Euro und mit Batteriestandzeiten von mehreren Jahren (mehr zum ZigBee-Standard lesen Sie im Beitrag ab 118).

Prof. Dr. Axel Sikora

Neuer Funk-Standard

Vernetzen mit ZigBee

Drahtlose Netze erschließen neue Anwendungsfelder. Im Nahbereich können nun Messaufnehmer, Schalter, Motoren, Lampen und Geräte vernetzt werden. Mit ZigBee wurde im Dezember ein neuer Standard verabschiedet, der viele Erwartungen weckt. CHIP informiert Sie über die Hintergründe.

Bei den immer weiter vordringenden drahtlosen Netzen macht eine neue Kategorie in zunehmendem Maße auf sich aufmerksam. Gab es bislang schon getrennte Funkanbindungen für Außenthermometer, Garagentoröffner, Rolladensteuerungen, Brandmelder oder Industrieanlagen, so versprechen standardisierte drahtlose Sensor-Aktor-Netzwerke (SANET) auf der Grundlage von Kurzstreckenfunk (Short-Range Wireless Networks, SRWN) einen großen Mehrwert für den Anwender. Es erscheint möglich, die Geräte von einer Zentrale, etwa einem PDA oder einem Notebook, zu steuern und zu vernetzen. Dabei erscheint auch die in dem Artikel ab 114 vorgestellte Vermaschung von Netzen als eine attraktive Variante, um das Reichweiten- und das Verlustleistungsproblem von In-House-Anwendungen zu entschärfen.

Dieser Beitrag konzentriert sich auf Techniken, Geräte und Installationen, die auf den jüngst veröffentlichten IEEE802.15.4- und ZigBee-Technologien basieren (mehr Informationen dazu finden Sie unter **www.ieee802.org/15/pub/SG4a.html** und **www.zigbee.org**).

GLOSSAR

IEEE802.15.4 Der IEEE-Standard für Nahbereichsfunknetze im 868-MHz- und 2,4-GHz-Bereich mit Datenraten von bis zu 250 KBit/s beschreibt die Layer 1 und 2 im OSI-Referenzmodell.

SANET (Sensor-Aktor-Netzwerke): Netzwerk etwa zwischen Datenaufnehmern und Steuergeräten.

SRWN (Short-Range Wireless Networks): Kurzstreckenfunk, der kostengünstige und verlustleistungsarme Funkmodule erlaubt.

WPAN (Wireless Personal Area Network): Netzwerk, das die Geräte im persönlichen Umfeld eines Nutzers drahtlos koppelt.

ZigBee Standard für Nahbereichsfunknetze, die auf IEEE802.15.4 aufbauen und standardisierte Mesh-Netzwerke und Anwendungsprofile verwenden.

Anwendungen und Technologien

Drahtlose Netze gewinnen immer mehr Verbreitung, da sie Flexibilität, Mobilität und Komfort vereinen und die Allverfügbarkeit von Rechnerressourcen im Sinne eines Ubiquitous Computing ein Stück näher bringen. Auf Grund der allerdings sehr viel unterschiedlicheren Anforderungen bei drahtlosen Netzen in Bezug auf Reichweite, Verlustleistungsaufnahme und (vor allem) Kosten ist an dieser Stelle noch keine „eierlegende Wollmilchsau" – wie das drahtgebundene Ethernet nach IEE802.3 – zu erkennen. Stattdessen ist weiterhin die Segmentierung in die klassischen Netzebenen zu beobachten.

Dabei spielen auch Technologien im untersten Kostenbereich eine besondere Rolle, da mit ihrer Hilfe viele Geräte und Anwendungen mit einer Netzwerkanbindung ausgestattet werden können, bei denen dies bislang kommerziell kaum möglich war. Man unterscheidet dabei insbesondere:

Wireless Personal Area Networks (WPAN), die wie das vor allem in der Consumer-Elektronik etabliert Bluetooth das Ziel haben, Peripheriegeräte drahtlos an eine zentrale Station anzuschließen.

Kurzstreckenfunknetze (Short-Range Wireless Networks, SRWN) beziehungsweise Sensor-Aktor-Netzwerke (SANET) adressieren vor allem den Bereich der Datenkommunikation zwischen Maschinen. Sie können dabei komplette und komplexe Netzarchitekturen realisieren.

Radio Frequency Identification (RFID) dient der Identifizierung von Objekten. Allerdings basieren die RFID-Tags meist auf passiven Transpondern und somit auf einer Punkt-zu-Punkt-Kommunikation mit einem aktiven Knoten (mehr zu RFID lesen Sie im Beitrag ab 42).

Dieser Bereich der kleinen und kleinsten Funksysteme wird, basierend auf einem sehr frühen Projekt an der UCSB, oft auch unter dem Schlagwort „Smart Dust" zusammengefasst (mehr Informationen finden Sie unter **http://robotics.eecs.berkeley.edu/~pister/SmartDust/**

IEEE802.15.4 und ZigBee

Die Anwendungen von SRWNs beziehungsweise SANETs reichen von der Industrie- und Automatisierungstechnik (Anlagensteuerung per Funk) über Spedition und Logistik (Güterüberwachung) sowie die Heim- und Gebäudeautomatisierung (kabelfreie Steuerung von Haushaltsgeräten, Klima- und Heizungsanlagen, Energieüberwachung), die Medizintechnik (drahtlose Patientendaten-Übertragung) bis hin zur Bedienung von Computer-Peripherie und Unterhaltungselektronik.

Um diese auch quantitativ sehr attraktiven Märkte mit einem herstellerübergreifenden Standard zu adressieren, erscheinen die bestehenden Lösungen wie IEEE802.11 (W-LAN) oder Bluetooth zu teuer, zu stromfressend oder zu unflexibel sind (siehe Tabelle auf 119).

So wurde bereits 1998 mit Vorarbeiten für einen eigenen Standard im HomeRF-Umfeld begonnen. Ende 2004 ist die Spezifikationsphase zu einem vorläufigen Abschluss gelangt. Dabei besteht die Protokollbeschreibung aus drei Teilen, die von unterschiedlichen Parteien entwickelt und bereitgestellt werden. **Der IEEE802.15.4** beschreibt die Bitübertragungs- und Sicherungsschicht (Layer 1 und 2), wurde im Oktober 2003 verabschiedet und steht unter der Adresse **www.ieee802.org/15/pub/SG4a.html** zum Download bereit. Erste Hardware- und Software-Produkte sind bereits verfügbar (mehr Informationen zu

diesen Produkten finden Sie unter **www.chipcon.com** und **www.freescale.com**).

Die Protokolle der Netzwerk- und Anwendungsschicht werden unter dem Marketing-Namen ZigBee zusammengefasst. Die Verabschiedung der Protokolle erfolgte nach einigen Irrungen und Wirrungen im Dezember 2004. Der Name ZigBee leitet sich übrigens von dem Zickzack-Tanz der Biene ab, die auf diese Weise ihren Artgenossen den Weg zur nächsten Nahrungsquelle mitteilt. In ähnlicher Weise sollen auch die Datenpakete im vermaschten Netz ihren Weg finden.

Spezifische Anwendungsprofile und -protokolle werden von den Systemherstellern beschrieben und von Anwendungsentwicklern umgesetzt.

Trotz des eigentlichen Ziels, einen einfachen Standard zu entwerfen, der kostengünstig zu realisieren ist, hat der Umfang der Systembeschreibungen erkleckliche Ausmaße angenommen. Insbesondere bei den ZigBee-Protokollen ist die Vielfalt der Betriebsoptionen beeindruckend. Man muss sich die Frage stellen, ob in der Praxis flexible Anpassbarkeit und Skalierbarkeit der Interoperabilität nicht doch entgegenstehen werden. Positiv ist jedoch zu vermerken, dass es gelungen ist, die Komplexität einer ausgewählten Realisierung gering zu halten. 26 Funktionsaufrufen (Primitives) im 802.15.4 stehen immerhin 131 Funktionsaufrufe im 802.15.1 (IEEE-Fassung von Bluetooth-MAC und -PHY) entgegen.

Die Auguren von IEEE802.15.4 und ZigBee wollen die folgenden Ziele erreichen:

Low Cost: Die Netzwerkkomponenten sollen preislich so günstig sein, dass sie in zahllose Anwendungen der oben beschriebenen Märkte Eingang finden können. Dabei gilt der einfache Grundsatz, dass die Anzahl der Anwendungen mit sinkenden Kosten steigt.

Low Power: Die Netzwerkkomponenten sollen so stromsparend sein, dass ein batteriegestützter Betrieb über mindestens mehrere Monate, möglichst sogar über mehrere Jahre sichergestellt werden kann.

Low Datarate: Für viele der oben genannten Anwendungen werden nur geringe Datenraten benötigt, was den Anforderungen sowohl in Bezug auf die Verlustleistungsaufnahme als auch in Bezug auf die Kosten entgegenkommt.

Mesh Networks: Die Netzwerkkomponenten sollen standardisiert sein. Auf diese Weise können über höhere Stückzahlen nicht nur niedrigere Herstellungskosten erreicht werden, sondern auch interoperable und interaktive Knoten realisiert werden. Dabei besteht der angestrebte Idealfall in der dynamischen Vernetzung aller vorhandenen Knoten: Wird über die Fernsteuerung der Ölbrenner im Keller gesteuert, sollen die Daten über den Brandmelder, die Kaffeemaschine und den Stromzähler weitergeleitet werden.

Bitübertragungsschicht

Die Bitübertragungsschicht stellt in Bezug auf die Funkschnittstelle verschiedene Varianten zur Auswahl. Im weltweit verfügbaren 2,4 GHz-ISM-Band sind 16 Kanäle mit einer maximalen Datenrate von 250 KBit/s vorgesehen. Darüber hinaus sind zwei weitere ISM-Bänder definiert: in Europa der Kanal bei 868,3 MHz mit 20 KBit/s und in USA/Pazifik zehn Kanäle mit 40 KBit/s zwischen 902 und 928 MHz.

Für die Übertragung im 2,4-GHz-Band wird ein sehr vereinfachtes Direct-Sequence-Spread-Spectrum-Verfahren (DSSS) eingesetzt. Das kann den Einfluss schmalbandiger Störer reduzieren, sodass man auf die Synchronisation in langen Powerdown-Phasen verzichten kann, wie sie beispielsweise bei dem bei Bluetooth eingesetzten Frequenzsprungverfahren (FHSS) notwendig wären.

Sicherungsschicht

Topologien: Der Standard IEEE-802.15.4 sieht mit Reduced Function Devices (RFD) und Full Function Devices (FFD) zwei Geräteklassen vor. Ein FFD kann mit RFDs oder anderen FFDs kommunizieren, während ein RFD nur mit einem FFD kommunizieren kann. Auf diese Weise können RFD-Funkknoten sehr einfach implementiert werden. Insbesondere ist auch eine Software-Realisierung auf einem kostengünstigen 8-Bit-Mikrocontroller möglich. Mit diesen beiden Geräteklassen können die grundlegenden Stern- und Peer-to-Peer-Topologien gebildet werden, die man als Personal Area Network (PAN) bezeichnet. In einem PAN erfüllt ein FFD als „PAN-Koordinator" Synchronisationsdienste durch das Versenden von Broadcast-Paketen (Beacons). In der Verschaltung ergibt sich ein Clustered Tree (vgl. die Info-Grafik aus dem Beitrag über Mesh-Netze auf 116).

Kanalzugriff: Der Kanalzugriff beim Standard IEEE 802.15.4 basiert grundsätzlich auf einem wahlfreien CSMA/CA-Verfahren, wie es auch vom W-LAN-Standard IEEE 802.11 bekannt ist. Dabei kann dieser auch erweitert werden, indem in einer so genannten Superframe-Struktur Zeitschlitze für zeitkritische Daten reserviert werden. Die Zuteilung dieser Zeitschlitze übernimmt der PAN-Koordinator. Auf diese Weise können dann insbesondere periodisch auftre- →

KNOW-HOW

Funktechniken im Systemvergleich

	IEEE802.11b	Bluetooth	IEEE802.15.4 & ZigBee
Batteriestandzeiten	Stunden	Wochen	Jahre
Materialkosten (u.U. ohne Host-Controller, ohne Software-Stack)	9 Dollar	6 Dollar	weniger als 3 Dollar
Reichweite (spezifiziert)	100 Meter	100 Meter	70 Meter
Roaming	möglich	nicht möglich	vermaschte, adaptive Netze als Zielvorstellung
Brutto-Datenrate	11 MBit/s	1 MBit/s	250 KBit/s
PC-Anbindung	unmittelbar gegeben	mittelbar gegeben	noch bereitzustellen
Komplexität	hoch	sehr hoch	mäßig

tende Kommunikationsströme (regelmäßige Sensor-Read-Outs) echtzeitmäßig übertragen werden.

Protokolle der Netzwerkschicht

Die Netzwerkschicht (NWK-Layer) ist die erste ZigBee-Schicht. Ebenso wie die im IEEE802.15.4 beschriebenen PHY- und MAC-Teilschichten ist sie in zwei nebeneinander angeordnete Bestandteile aufgeteilt. Die Network Layer Data Entity (NLDE) dient dem Transport der Daten zwischen zwei Endstationen. Die Network Layer Management Entity (NLME) übernimmt die Verwaltung der Netzwerke.

Die Wegefindung (Routing) ist ein wesentlicher Bestandteil der NWK-Schicht. Dies gilt um so mehr, als ZigBee ja ursprünglich mit dem Ziel angetreten ist, auch Mesh-Networking und damit eine leistungsfähige, dynamische und adaptive Transportfunktionalität über Relaisstationen zu unterstützen. Von dem ursprünglichen Ziel einer allgemeingültigen Unterstützung mit Wegeoptimierung und Lastverteilung ist man auf Grund der übergroßen Komplexität der Routing-Algorithmen wieder ein wenig abgerückt und unterstützt zum einen Routing mit Hilfe hierarchischer Adressierung und zum anderen ein tabellenbasierendes Routing, sodass kleine adaptive Netzwerke aufgebaut werden können. Für große Systeme mit mehreren hundert oder tausend voll vermaschten Stationen sind die vorgestellten Ideen kaum tauglich. Dies ist vor dem Hintergrund der begrenzten Ressourcen in den Knoten verständlich.

Protokolle der Anwendungsschicht

Ähnlich wie Bluetooth versucht auch ZigBee, die Spezifikation bis auf Anwendungsebene durchzuführen. Insbesondere werden auch Anwendungsprofile definiert, mit denen eine herstellerübergreifende Interoperabilität gewährleistet werden soll. Im Vergleich mit Bluetooth lassen sich vor allem zwei Eigenschaften hervorheben:

Mit der Definition sehr detaillierter Anwendungsprofile, beispielsweise Switch Remote Control (Lichtschalter) oder Dimming Light Controller (Dimmer), setzt sich ZigBee allerdings der gleichen Gefahr wie Bluetooth aus, das bereits über viel zu viele Anwendungsprofile verfügt. Die Interoperabilität zwischen ähnlichen Geräten ist dadurch in Frage gestellt.

Die besten ZigBee-Tipps im Web

Alles über das ZigBee-Projekt → www.zigbee.org
Webseite der ZigBee-Allianz mit zahlreichen Artikeln und Hintergrundinformationen. Auf diesen Seiten will die Allianz auch ab März den ZigBee-Standard veröffentlichen.

Alles über IEEE 802.15.1 → www.bluetooth.org
Webseite der Bluetooth Special Interest Group (BSIG). Nach kostenloser Anmeldung stehen die Standards und zahlreiche weitere Materialien und Berichte zur Verfügung.

Produkte nach dem ZigBee-Standard → www.chipcon.com
Webseite des norwegischen Chip-Herstellers ChipCon, der sich auf die Entwicklung von RF-Chips spezialisiert hat. Dort finden sich neben Datenblättern auch Hintergrundinformationen und Application Notes.

Produkte nach dem ZigBee-Standard → www.freescale.com
Webseite der ehemaligen Halbleitertochter von Motorola. Unter www.freescale.com/webapp/sps/site/overview.jsp?nodeId=02XPgQhHPRjdyB findet sich ein umfangreiches Verzeichnis zu IEEE 802.15.4 und ZigBee-Aktivitäten.

Alles über IEEE 802.11 → http://grouper.ieee.org/groups/802/11/index.html
Webseite der 802.11-Arbeitsgruppe in der Standards Association des IEEE mit aktuellen Diskussionen und Entwicklungen (mit geschütztem Mitgliederbereich).

Alles über IEEE 802.15.4 → www.ieee802.org/15/pub/ SG4a.html
Webseite der 802.15.4-Arbeitsgruppe in der Standards Association des IEEE mit aktuellen Diskussionen und Entwicklungen (mit geschütztem Mitgliederbereich).

Alles über SmartDust → http://robotics.eecs.berkeley.edu/~pister/SmartDust/
Webseite zum Smart-Dust-Projekt der University of California in Berkeley, dem Vorläufer von ZigBee.

ZigBee hat aber auch aus den Erfahrungen von Bluetooth gelernt. Denn nicht nur der gesamte Protokollstapel, sondern auch die Anwendungsschicht ist sehr viel modularer aufgebaut, sodass eine feinere Skalierung des Standardisierungsgrades möglich ist. Insbesondere ist auch die Einbindung proprietärer Anwendungsprofile mit standardisiertem Aufbau vorgesehen.

Die Kehrseite dieses modularen Ansatzes ist eine ziemlich hohe Komplexität des gesamten Aufbaus mit einer recht großen Anzahl von Schnittstellen.

Ausblick

Die vorgestellten Technologien können drahtlosen Netzen in einem weiteren Anwendungsbereich zum Durchbruch verhelfen. Zahlreiche Produktentwicklungen sind auf den Weg gebracht, sodass bereits in den nächsten Monaten mit ersten Serienprodukten zu rechnen ist. Der immense Mehrwert der Standardisierung wird erst bei einer weiten Verbreitung deutlich werden und dann andere und proprietäre Ansätze verdrängen. Prof. Dr. Axel Sikora

KNOW-HOW

Drahtlose Netze eröffnen neue Netzwerkebenen

	drahtlose Netzwerke		drahtgebundene Netzwerke
RFID	passive Transponder		nicht abgedeckt
SRWN	802.15.4 & ZigBee, proprietäre Lösungen		nicht abgedeckt
WPAN	Bluetooth		nicht abgedeckt
WLAN	IEEE802.11/WiFi (Home RF, HiperLAN/2)	LAN	IEEE802.3
WMAN	IEEE802.16/WiMax, proprietäre Lösungen	MAN	IEEE802.3, FDDI
WWAN	GSM/GPRS, UMTS	WAN	IEEE802.3, X.25, Frame Relay, ATM

Netzwerkstatus überwachen

Transparenz fürs W-LAN

Installation und Einrichtung von Funknetzen ist heute dank vorkonfigurierter Hardware verhältnismäßig leicht. Bei kleinen Netzen, die meist aus nur wenigen Stationen bestehen, geschieht dies in der Regel fast automatisch. Um so wichtiger ist es, das W-LAN bei der Arbeit im Auge zu behalten. Einige Windows-Tools helfen Ihnen dabei.

Ihr drahtloses lokales Netzwerk funktioniert wie ein Ethernet, auch wenn es sich beim Übertragungsmedium nicht um ein Kupferkabel handelt. Windows XP verfügt in bescheidenem Maße über einige Netzwerk-Diagnosetools. Die Wichtigsten stellt Ihnen dieser Beitrag vor.

Statusmeldungen abfragen

Als Verwalter eines Netzwerks ist es immer gut, die Aktivitäten im Wireless LAN zu überwachen. Am einfachsten geht das mit einer Statusmeldung. Wenn Sie die Netz-Aktivitäten während der aktuellen Sitzung überwachen wollen, öffnen Sie unter Windows XP die Netzwerkumgebung.

1. Klicken Sie im Fenster „Netzwerkumgebung“ auf die Option „Netzwerkverbindungen anzeigen“.

2. In diesem Ordner ist ein Verbindungssymbol mit dem Benutzernamen im Ordner „Netzwerkverbindungen“ aufgeführt, sobald die Benutzer eine Verbindung aufbauen. Klicken Sie mit der rechten Maustaste auf die „LAN-Verbindung“ und wählen Sie die Option „Status“. Daraufhin werden Ihnen die folgenden Informationen angezeigt:

Verbindungsstatus

Dauer einer Verbindung.

Übertragungsrate

Anzahl der Bytes, die während einer Verbindung gesendet und empfangen wurden, außerdem die zugehörige Komprimierung und die Fehlerstatistik

die Diagnosetools für eine Verbindung (falls vorhanden), beispielsweise „Windows Netzwerk-Ratgeber“, „TCP/IP-Autoping“ und „TCP/IP Windows IP-Konfiguration“. Diese Tools werden durch die Anbieter explizit unter Windows XP registriert, unabhängig davon, ob sie von Microsoft oder einem anderen Anbieter bereitgestellt wurden.

3. Aktivieren Sie die Registerkarte „Details“. Dort erhalten Sie weitere Informationen über die aktuelle Netzwerkverbindung.

4. Schließen Sie das zuletzt geöffnete Fenster und klicken Sie auf die Schaltfläche „Eigenschaften“.

5. Klicken Sie nun auf den Button „Einstellungen“. Dort finden Sie die Einstellungen zur Windows-XP-Firewall und zur gemeinsamen Nutzung der Internet-Verbindung.

Netzwerkmonitor automatisch aktivieren

Unter Windows XP ist es möglich, den Statusmonitor automatisch zu aktivieren. Dazu muss die Verbindung aktiv sein.

1. Klicken Sie mit der rechten Maustaste auf die Verbindung und wählen Sie die Option „Eigenschaften“ aus dem Kontextmenü.

2. Aktivieren Sie dann das Kontrollkästchen „Symbol bei Verbindung im Infobereich der Taskleiste anzeigen“.

Wenn Sie anschließend mit der Maus über das Netzwerksymbol in der Windows-Taskleiste fahren, wird Ihnen die aktuelle Übertragungsrate angezeigt. Ein Klick auf das Symbol öffnet das Statusfenster.

Die Netzwerk-Auslastung anzeigen

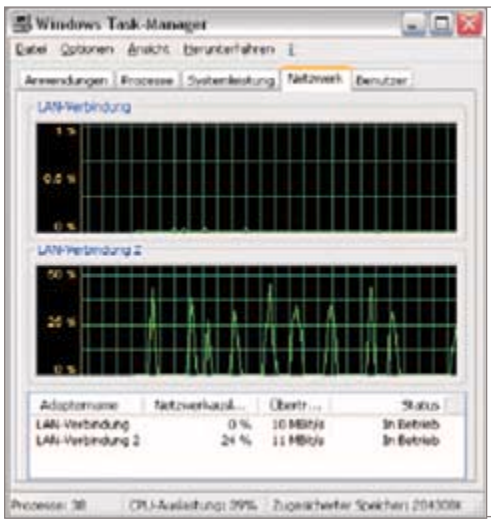
Den Windows-XP-Taskmanager können Sie auch dazu nutzen, um sich die Auslastung eines Netzwerks anzeigen zu lassen. So gehen Sie vor:

1. Drücken Sie die Tasten [Strg]+[Alt]+[Entf].

2. Aktivieren Sie im Taskmanager die Registerkarte „Netzwerk“.

Statusmeldungen der Netzwerk-Software

Auch die Netzwerk-Software, also die Software, die mit dem Access Point oder mit der Netzwerkkarte geliefert wurde, kann Ihnen in den meisten Fällen den Status der Netzwerk-Verbindung melden. Häufig ist dieses Feature mit einer Diagnose-Funktion gekoppelt. Sie starten die Software durch einen Dop-


Windows Task-Manager
Datei Optionen Ansicht Beenden
Anwendungen Prozesse Systemleistung Netzwerk Benutzer
LAN-Verbindung
LAN-Verbindung 2
Adaptername Netzwerkauslastung Übertragungsrate Status
LAN-Verbindung 0 % 10 MBit/s In Betrieb
LAN-Verbindung 2 24 % 11 MBit/s In Betrieb
Prozesse: 38 CPU-Auslastung: 99% Zugesicherter Speicher: 204308k

WAS LÄUFT? **Der Taskmanager von Windows XP zeigt Ihnen auf der Registerkarte „Netzwerk“ die Auslastung Ihres W-LANs an.**

CHIP → DVD-CODE W-LAN, Administration

- **W-LAN-Toolkit** Auf Heft-DVD finden Sie die besten Tools für drahtlose Netze, darunter den Network Stumbler, Fake-AP für Linux oder den Mac-Sniffer iStumbler (Code: W-LAN).
- **Analyse-Tools** Top-Tools für Analyse und Diagnose im LAN sind Ethereal, der Portscanner NmapWin, Look@LAN und der Profilmanager NetSetMan (DVD-Code: Administration).

pelklick auf das entsprechende Symbol oder durch einen Klick auf das Symbol in der Windows-Taskleiste.

LAN-Diagnose mit Bordmitteln und Tools

Es gibt Schwiegermütter, das Finanzamt – und Netzwerk-Probleme, alles Dinge, die einen Menschen leicht zur Verzweiflung treiben können. Zumindest bei den Netzwerk-Problemen bietet Windows XP mit Bordmitteln eine erste Hilfestellung. Den Rest erledigen leistungsfähige Tools.

Einige Probleme im Netzwerk lassen sich oft schon mit Windows XP lösen. Das Betriebssystem verfügt über einige Netzwerkdiagnose-Funktionen, die beim Erkennen von Netzwerk-Problemen helfen. Der Netzwerkdiagnose-Assistent unterstützt Sie beim Aufspüren auch komplizierter Fehler und bietet Strategien zur Problembehandlung – nicht nur für Profis, sondern auch für Benutzer mit weniger Erfahrungen in der Netzwerk-Administration. Die folgenden Beispiele funktionieren sowohl in einem leitungsgebundenen Netzwerk, als auch in einem Wireless LAN.

Netzwerk-Diagnose leicht gemacht

Wenn Ihr lokales W-LAN Probleme bereitet, können Sie zunächst einmal ein Diagnoseprogramm durch das Netzwerk schicken, das das System nach allen Regeln der Kunst durchcheckt. Die Fehlersuche starten Sie mit Hilfe des Netzwerkdiagnose-Assistenten. Dieser XP-Assistent listet die Informationen über das Netzwerk und die einzelnen Rechner. Als Administrator haben Sie die Möglichkeit, das lokale Netzwerk nach Fehlerquellen zu durchsuchen und Testverfahren, beispielsweise Verfügbarkeits-Checks durchzuführen.

1. Klicken Sie auf den Start-Button und wählen Sie die Option „Hilfe und Support".
2. Im Fenster „Hilfe- und Supportcenter" klicken Sie auf die Option „Tools zum Anzeigen von Computerinformationen".
3. Auf der linken Fensterseite finden Sie unter der Überschrift „Tools" die Option „Netzwerkdiagnose". Klicken Sie darauf.
4. Klicken Sie anschließend auf „System überprüfen", um die Diagnose zu starten.

Das Betriebssystem testet nun die Netzwerkverbindungen und teilt Ihnen mit, wo Verbindungsfehler aufgetreten sind.

Eine Netzwerkverbindung reparieren

Gelegentlich kann die Netzwerkkonfiguration des PCs in einen Zustand übergehen, der die Netzwerkkommunikation behindert. Das lässt sich jedoch durch eine Reihe von allgemeinen Verfahren, etwa das Erneuern der IP-Adresse und der DNS-Namensregistrierung, korrigieren. Damit Sie diese Schritte nicht manuell vorzunehmen brauchen, hat Microsoft eine Reparatur der Netzwerkverbindung in das Kontextmenü aufgenommen.

Sie finden diese Reparatur-Option im Statusfenster der Netzwerkverbindung. Die Verbindung wird getestet und gegebenenfalls in einen betriebsbereiten Zustand zurückgesetzt. Und so gelangen Sie dort hin:

1. Klicken Sie auf den Start-Button und wählen Sie die Optionen „Netzwerkumgebung" und „Netzwerkverbindungen anzeigen".
2. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung und wählen Sie die Option „Status".
3. Aktivieren Sie die Registerkarte „Netzwerkunterstützung" und klicken Sie auf die Schaltfläche „Reparieren". Die Auswahl dieser Option löst eine Reihe von Schritten aus, die sehr wahr- →

ANALYSE- UND DIAGNOSE-TOOLS — **DVD-CODE** Administration

Name	Adresse	Lizenz	Funktion
Ethereal	www.ethereal.com	Freeware	Netzwerkprotokoll-Analysator mit der Möglichkeit, Daten im laufenden Netzwerkbetrieb zu speichern und zu analysieren.
IPDog	www.thbi.de	Shareware	Das Programm zeigt dem Benutzer alle ein- und ausgehenden Verbindungen sowie Zugriffe auf Ports an und stellt die Daten übersichtlich in einer Liste dar. Neben Quell- und Zieladresse werden die Anzahl der Zugriffe, Portnummer, Paketgröße und das verwendete Protokoll angezeigt. Bei der Portauflistung gibt das Programm zusätzlich Portnamen und -beschreibung an, falls diese bekannt sind.
Nmap Win	www.insecure.org	Freeware	Dieser Scanner kennt die gefährlichen Ports für potenzielle Angreifer und überprüft, welche Ports offen sind. Anfänger erhalten nützliche Informationen über die verschiedenen Ports.
Look@LAN	www.lookatlan.com	Freeware	Netzwerk-Monitor zur Überwachung und Analyse eines Netzwerks mit Alarmfunktion, ausführlicher Statistik mit Diagrammen und sehr benutzerfreundlicher Oberfläche.
Network Administrator's Toolkit	www.alchemy-lab.com	Shareware	Network Administrator's Toolkit besteht aus einem Tool, das sämtliche Hard- und Softwarekomponenten des Netzwerks in einer exportfähigen Bestandsliste aufführt. Ein weiteres Tool überwacht die Systemleistung und benachrichtigt bei Störungen den Administrator. Dieser hat die Möglichkeit, die Netzwerk-PCs per Remote Control fernzusteuern.
NetSetMan	www.itecnix.com	Freeware	NetSetMan ist ein Netzwerkverwaltungs-Programm und richtet sich vor allem an mobile PC-Anwender, die täglich mit dem Notebook unterwegs sind. Das Programm verwaltet bis zu fünf Profile.
PCTEL	www.pctel.com	Shareware	Werkzeug für das Verwalten von Zugriffen auf Wi-Fi-(802.11-)Netze im Unternehmen, im Heimnetzwerk oder via öffentlicher Wi-Fi-Hotspots.
TrafMeter	www.trafmeter.com	Shareware	IP- und Netzwerküberwachungstool zum Aufzeichnen und zur Analyse der IP Pakete und des Datenverkehrs mit flexibler Filtertechnik. Die Überwachung von einzelnen Hosts, ganzen Subnetzen oder Gruppen von Hosts ist möglich.

scheinlich das Kommunikationsproblem lösen und mit Sicherheit keine ernsten Probleme verursachen.

User Migration Tool einsetzen

Unter Windows XP können Sie als Systemadministrator Einstellungen und Dateien von einem Netzwerk-Computer auf weitere PCs übertragen. Wenn Sie etwa einen neuen PC in das Netzwerk aufnehmen wollen, ist es mit diesem Programm möglich, die anwenderspezifischen Daten sowie die individuellen Einstellungen auf den neuen Rechner zu übertragen. Das Tool arbeitet auch mit den Betriebssystemen Windows 95, 98, NT 4.0, Me und 2000 zusammen. So aktivieren Sie es:

1. Klicken Sie auf den Start-Button und wählen Sie die Optionen „Alle Programme | Zubehör | Systemprogramme".

2. Starten Sie den Assistenten durch die Option „Übertragen von Dateien und Einstellungen".

3. Lesen Sie die Informationen aufmerksam und klicken Sie anschließend auf den Button „Weiter".

4. Wählen Sie den Quell- und Zielcomputer aus und geben Sie an, auf welchem Wege die benutzerdefinierten Einstellungen übertragen werden sollen. Nachdem Sie alle Angaben gemacht haben, klicken Sie auf „Fertigstellen".

Die entsprechenden Daten werden nun über das lokale Netzwerk auf den Zielrechner übertragen. Darüber hinaus ist es möglich, die Einstellungen auf Diskette oder beispielsweise auf eine CD-ROM zu speichern und danach die Dateien auf den Ziel-PC zu übertragen. Sämtliche benutzerdefinierten Einstellungen und Dateien sind anschließend auf dem Zielrechner und dem Quell-PC identisch und funktionsfähig.

Weitere Diagnose-Tools

Neben den Tools aus der Windows-Umgebung gibt es eine ganze Fülle hilfreicher Test- und Diagnose-Software, mit denen man eine Menge interessanter Informationen über verschiedene Komponenten, Systeme und Zustände in einem Netzwerk in Erfahrung bringen kann. Die im Kasten „Analyse- und Diagnose-Tools" auf 123 vorgestellten Programme dienen in erster Linie der Diagnose von Netzwerk- und Internet-Verbindungen. Software dieser Art bietet oft einen großen Funktionsumfang – vom klassischen „Ping" über WhoIs-Abfragen bis hin zur kompletten Protokollierung des Datenflusses von TCP/IP-Verbindungen. Mit Hilfe dieser Tools können Sie nicht nur nützliche Informationen sammeln, oft helfen sie auch bei der Ermittlung möglicher Schwachstellen des Netzwerk-Traffics.

TCP/IP-Tools unter Windows XP

Zur Verwaltung des Netzwerks und zur Netzwerksicherheit sind gute TCP/IP-Kenntnisse von Vorteil. Unter Windows XP gibt es eine Reihe grundlegender TCP/IP-Tools, die größtenteils von Windows NT/2000 stammen. Diese Programme können Sie von der Kommandozeile starten, aber auch vom Diagnose-Assistenten aufrufen. Die TCP/IP-Tools gelten für das Internet ebenso wie für lokale Netzwerke, in denen das TCP/IP-Protokoll verwendet wird. Die wichtigsten Verwaltungs- und Diagnose-Tools stellen wir Ihnen auf den nächsten Seiten vor.

Ping: Reaktionszeit messen

Ping steht für „Packet Internet Groper" (engl. für „Grapscher"); dabei handelt es sich um ein Programm, das die Reaktionszeit von Servern misst. Ein Rechner sendet ein Signal und wartet auf ein Echo. Danach wird die verstrichene Zeit (Round-Trip-Time) in Millisekunden und die Zahl der unterwegs verlorenen Datenpakete angezeigt. Ping kann auf diese Weise auch ermitteln, ob ein Server überlastet ist.

In Ihrem lokalen Netzwerk können Sie Ping benutzen, um die Funktionsfähigkeit einer Netzwerkverbindung zu testen. Das Tool ist für manuelle Testzwecke konzipiert und sollte während des normalen Betriebs nicht in automatisch ablaufenden Scripten eingesetzt werden. Am besten starten Sie das Programm über die Kommandozeile. Die genaue Syntax wird Ihnen durch folgenden Befehl angezeigt:

```
ping /h
```

Statt der IP-Adresse können Sie auch den Namen des Rechners angeben, den Sie „anpingen" wollen. Bevor Sie das Tool einsetzen, sollten Sie zunächst einen Ping an den eigenen Rechner (127.0.0.1) absetzen, um sicherzustellen, dass die eigene Netzwerkkarte richtig arbeitet. Danach können Sie sich von Station zu Station durchpingen.

Für Ihr lokales Netz könnte das so aussehen:

```
ping 192.168.0.1
```

oder

```
ping <Rechnername>
```

Das Ergebnis erscheint sofort.

Bekommen Sie keine Antwort, überprüfen Sie zunächst die eingegebene Adresse oder den Rechnernamen.

Stimmt die Adresse oder der Name und Ping bekommt trotzdem keine Antwort, obwohl Sie den anderen Computer in Windows sehen können, sollten Sie in der Netzwerkumgebung unter „Netzwerkverbindung" | Eigenschaften" sicherstellen, dass TCP/IP an die Netzwerkkarte „gebunden" ist.

PROFI-TIPPS

LAN-Diagnose professionell

Diagnose per Kommandozeile Der XP-Diagnose-Assistent lässt sich auch über „Start | Ausführen" aufrufen. Geben Sie danach den Befehl „netsh diag gui" ein. XP zeigt Ihnen nun ein Startfenster, in dem Sie die Testoptionen festlegen können.

TCP/IP reparieren Unter Windows 2003 Server ist eine Deinstallation von TCP/IP nicht möglich, um es etwa durch eine Neuinstallation wieder sauber aufzusetzen. Dafür können Sie jedoch die IP-RESET-Funktion des Tools netsh verwenden. Starten Sie das Tool mit: „netsh int ip resetlog.txt". In der Datei „resetlog.txt" können Sie das Protokoll des Resets nachlesen.

Firewall überprüfen Sollte im Netzwerk etwas nicht funktionieren, kann es auch an einer Firewall liegen. Häufig wird vergessen, dass eine Firewall aktiv ist und unter Umständen den Verkehr blockiert. Besonders ZoneAlarm macht sich oft nicht bemerkbar. Daher: Schalten Sie bei Problemen die Firewall probeweise einmal ab.

Fehlernummer enttarnen Bei einem Verbindungsaufbau zeigt das DFÜ-Netzwerk gelegentlich eine Meldung mit Fehlernummer. In der Knowledge Base von Microsoft (support.microsoft.com) sind unter der Nummer 163111 alle Fehlercodes des Remote Access Services gelistet.

Die besten Tools für drahtlose Netzwerke

Wie bei Kabelnetzen gibt es auch bei W-LANs Diagnoseprogramme, etwa für folgende Aufgaben:
Ursachenermittlung bei Fehlfunktionen
Messungen zur Verifizierung von Versorgungsbereichen
Ermittlung von Sicherheitslücken

Neben recht kostspieligen kommerziellen Diagnose-Tools gibt es eine Reihe von Freeware-/Shareware-Tools mit teilweise erstaunlichem Funktionsumfang. Es liegt auf der Hand, dass solche Programme auch immer großes Missbrauchspotenzial besitzen. Was dem einen bei der Analyse und Fehlersuche hilft, kann ein anderer ebensogut zu Spionage- und Sabotagezwecken nutzen.

WINDOWS

Name	Adresse	Eigenschaften
AiroPeek	www.wildpackets.com/products/airopeek	Software für 802.11b-Netzwerke, die die Protokolle TCP/IP, AppleTalk, NetBEUI und IPX unterstützt. Das Programm misst Performance und Signalstärke und bietet Informationen über Channels und Sicherheitslücken.
CEniffer	www.epiphan.com/products_ceniffer.html	Network-Analyzer für den Pocket-PC, der Informationen über Status und Aktivitäten im Netzwerk liefert.
Network Stumbler/ MiniStumbler	www.netstumbler.com	Wohl bekanntestes Tool zum Finden von W-LANs, das SSID, Channel, WEP-Option, Signalstärke und anderes anzeigt. In Zusammenarbeit mit GPS kann die genaue Position eines Access Points ermittelt werden. MiniStumbler läuft auf Pocket-PCs.
Stumbverter	www.sonar-security.com	Dieses Programm bietet die Möglichkeit, Network Stumbler-Dateien in das Programm MapPoint 2002 von Microsoft zu importieren. Hinzugefügt werden können MAC-Adressen und Notizen.

LINUX/UNIX

Name	Adresse	Eigenschaften
AirTraf	http://airtraf.sourceforge.net/index.php	AirTraf kann Pakete mitsniffen und auch dekodieren. Außerdem hilft die Software beim Aufspüren von Access Points. Die empfangenen Daten können in einer Datenbank abgelegt werden, auf die mit verschiedenen Tools zugegriffen werden kann.
Wireless AP-Utilities	ap-utils.polesye.net/	Tools zum Managen von Access Points unter Unix, Linux, FreeBSD, NetBSD und AIX via SNMP-Protokoll
FakeAP	www.blackalchemy.to/Projects/fakeap/fake-ap.html	Hervorragendes Programm zur Erhöhung der Sicherheit in einem W-LAN. Durch FakeAP werden 53.000 verschiedene Access Points vorgetäuscht. So dauert es für Programme wie Network Stumbler einfach zu lange, alle verfügbaren Access Points durchzuprobieren.
Freeswan	www.freeswan.org	IPsec unter Linux – die wahrscheinlich sicherste Art, Daten über ein W-LAN zu übertragen.
Kismet	www.kismetwireless.net	Netzwerk-Sniffer für 802.11b-W-LANs zum Mithören des Traffics
Mognet	node99.org/projects/mognet/	OpenSource-Wireless-Sniffer/Analyzer, der in Java programmiert wurde. Ursprünglich für den Compaq iPAQ geplant, läuft er auch auf Desktop-Systemen.
SSIDsniff	www.bastard.net/~Ekos/wifi/	Kleines Tool zum Finden von Access Points und zum Speichern von Netz-Traffic mit Konfigurationsskript. Unterstützt werden Cisco Aironet und verschiedene Prism2-Karten.
WellenReiter	www.remote-exploit.org	Perl-Programm, das es erleichtert, 802.11b-Netzwerke auszuforschen. Der Scanner kann Access Points, Networks und Ad-hoc systeme ausfindig machen. Broadcasting- sowie Non-Broadcasting-Netzwerke lassen sich automatisch aufspüren.
WEPCrack	wepcrack.sourceforge.net	Perl-Scripts zum Auslesen und Knacken des WEP-Keys, empfehlenswert zum Testen der eigenen Sicherheitseinstellungen
Wireless Security Auditor	researchweb.watson.ibm.com/gsal/wsa/	Tool aus dem IBM-Labor, das auf dem Linux-Betriebssystem von iPAQs läuft. Das Programm sucht automatisch nach schlechter Sicherheitskonfiguration, um Netzwerk-Administratoren Sicherheitsprobleme aufzuzeigen.

APPLE MACINTOSH

Name	Adresse	Eigenschaften
EtherPEG	www.etherpeg.org/	Tool zum Abhören des Netzwerkverkehrs
iStumbler		Kleines Tool zum Aufspüren von Funknetzwerken
KisMAC		Stumbler für Mac-OS X, der Funknetzwerke findet und die W-LAN-Karte in den Monitor-Modus versetzt. Weil keine Requests gesendet werden, arbeitet die Software unsichtbar für den W-LAN-Betreiber.
MacStumbler	www.macstumbler.com	Ähnliches Programm wie Network Stumbler (Windows) oder Kismet (Linux), funktioniert aber nur mit Apple-Airport-Karten.
Viha Wireless Tools	www.dopesquad.net/security/	Sammlung unterschiedlicher Tools für WLANs

→

Bekommen Sie ein Timeout oder keine Antwort, kann auch eine Störung im Netzwerk vorliegen. Überprüfen Sie alle Einstellungen und gegebenenfalls die Kabelverbindungen zu dem betroffenen Netzwerk-Rechner.

Der Befehl ping setzt ICMP-Echo-Anforderungen und Echo-Antworten (Internet Control Message Protocol) ein. Durch Paketfilterrichtlinien für Router, Firewalls oder andere Typen von Sicherheitsgateways kann die Weiterleitung von solchem Datenverkehr verhindert werden.

Ein Rechner, der zumindest ein Datenpaket als empfangen meldet, ist online. Lange Antwortzeiten oder verlorene Datenpakte deuten darauf hin, dass der Rechner überlastet ist.

Tracert: Fehler lokalisieren

Mit dem Befehl tracert haben Sie die Möglichkeit, die Anzahl der Hops zwischen einem System und einem Zielsystem zu ermitteln. Das Tool geht also einen Schritt weiter als Ping und hilft Ihnen, wenn Sie herausfinden wollen, an welcher Stelle des Weges im Netzwerk zum Bestimmungsort eine LAN-Verbindung fehlerhaft ist.

Geben Sie im Konsolenfenster den Befehl

```
tracert <IP-Adresse>
```

oder

```
tracert <Computername>
```

ein. Die vollständige Aufrufsyntax erhalten Sie durch die Eingabe von

```
tracert /?
```

Wenn Sie als Zielangabe eine Web-Adresse eintippen, bekommen Sie als Ergebnis die zugehörige IP-Adresse angezeigt.

Ipconfig: IP-Konfiguration ermitteln

Auch dieser Befehl hilft Ihnen, die TCP/IP-Konfiguration schnell in Erfahrung zu bringen. Umsteiger von Windows 98 oder 2000 werden den Befehl winipcfg vermissen. Das Tool ipconfig unter Windows XP arbeitet ähnlich, allerdings ohne grafische Oberfläche. Durch den Befehl

```
ipconfig /h
```

können Sie sich die vollständige Aufrufsyntax des Befehls anzeigen lassen. Öffnen Sie das Fenster für die Eingabeaufforderung und geben Sie den Befehl

```
ipconfig
```

ein. Das Ergebnis mit der IP-Konfiguration Ihres Netzwerks kommt postwendend auf den Bildschirm.

Beim Aufruf ohne weitere Parameter zeigt ipconfig die IP-Adresse, die Subnetzmaske und einen Standard-Gateway für alle Netzwerkadapter an. Ist der Rechner mit mehreren Netzwerkkarten ausgestattet, geben Sie stattdessen

```
ipconfig /all
```

in das Konsolenfenster ein.

Net view: Freigaben überprüfen

Durch den Befehl net view werden die Datei- und Druckerfreigaben eines Computers unter Windows XP überprüft, indem er eine temporäre Verbindung herstellt. Wenn keine Datei- oder Druckerfreigaben auf dem angegebenen Computer eingerichtet wurden, gibt das Tool die Fehlermeldung „Es sind keine Einträge in der Liste“ aus.

Geben Sie in der Eingabeaufforderung den Befehl

```
Net view <IP-Adresse>
```

oder

```
net view <Computername>
```

ein. Das Ergebnis sehen augenblicklich.

Wenn der Befehl net view fehlschlägt und die Fehlermeldung „Systemfehler 5 ist aufgetreten“ oder die Meldung „Zugriff verweigert“ erscheint, sollten Sie überprüfen, ob Sie berechtigt sind, auf den Rechner zuzugreifen.

Zeigt das Tool dagegen die Fehlermeldung „Systemfehler 53 ist aufgetreten“ an, ist auf dem angesprochenen Computer möglicherweise die „Datei- und Druckerfreigabe für Microsoft-Netzwerke“ nicht aktiviert. Überprüfen Sie aber auch die korrekte Eingabe des Computernamens, die Funktionstüchtigkeit des Computers, der den Befehl ausführt, sowie die Funktionstüchtigkeit aller Gateways (Router) zwischen dem angesprochenen PC und dem Computer, der den Befehl ausführt.

Net view nimmt an, dass Sie in Ihrem Netzwerk nur das TCP/IP-Protokoll verwenden. Wenn Sie dort auch andere Protokolle einsetzen, etwa NWLink, ein IPX/SPX/NetBIOS-kompatibles Transportprotokoll, funktionieren net-view-Befehle eventuell

PROFI-TIPP

Mehr Tempo im Netzwerk

Überwachen und die TCP/IP-Tools einsetzen, ist die eine Seite der Medaille. Auf der anderen Seite gibt es die Möglichkeit, ein Netzwerk ein bisschen schneller zu machen. Ob Sie ein Unternehmensnetzwerk oder ein kleines Heimnetzwerk betreiben – etwas Tempospeigerung ist immer drin.

Zunächst sollten Sie sicherstellen, dass Sie die neuesten Treiber für Ihre Netzwerk-Adapter verwenden. Besonders die Windows-eigenen Treiber neigen ziemlich häufig zu Verbindungsabbrüchen oder sind instabil.

Den aktuellen Treiber finden Sie auf der Homepage des Karten-Herstellers. So kann eine Überprüfung ablaufen:

1 Klicken Sie auf den Start-Button und wählen Sie die Option „Netzwerkumgebung“.

2 Lassen Sie sich die Netzwerkverbindungen anzeigen und klicken Sie mit der rechten Maustaste auf die Netzwerkkarte, deren Treiber Sie überprüfen möchten.

3 Wählen Sie mit einem Mausklick die Option „Eigenschaften“ aus.

4 Klicken Sie anschließend auf die Option „Konfigurieren“.

5 Aktivieren Sie im neuen Fenster die Registerkarte „Treiber“. Dort können Sie die Versionsnummer des installierten Treibers ermitteln.

6 Klicken Sie auf „Aktualisieren“, wenn Sie einen neuen Treiber installieren wollen. Geben Sie den Pfad zu diesem Treiber an und folgen Sie den Schritten des Assistenten.

7 Alternativ stellen Sie eine Online-Verbindung zur Homepage Ihres Netzwerkkarten-Herstellers her. Finden Sie dort eine neuere Version, laden Sie diese herunter und installieren Sie sie.

Bei vielen No-Name-Karten ist es schwierig, die Homepage des Herstellers zu finden. Dann hilft nur noch ein Blick in die Systemsteuerung oder auf die Netzwerkkarte, um festzustellen, wer den Chipsatz hergestellt hat. Suchen Sie mit einer Suchmaschine nach den Online-Seiten des Herstellers. Meist finden Sie dann eine Adresse, wo Sie den neuen Treiber herunterladen können.

auch dann korrekt, wenn Probleme mit der Auflösung von Namen und dem Herstellen von Verbindungen mit TCP/IP auftreten. Der Versuch, eine net view-Verbindung herzustellen, wird bei allen installierten Protokollen unternommen. Kann die net-view-Verbindung mit TCP/IP nicht hergestellt werden, unternimmt XP den Versuch, eine net-view-Verbindung mit Hilfe des IPX/SPX/NetBIOS-kompatiblen Transportprotokolls NWLink herzustellen.

Netstat: Port-Status anzeigen

Netzwerk-Administratoren, die sich mit diesem Tool sehr gut auskennen, können damit schnell herausfinden, welche Ports auf einem System verwendet werden. Netstat zeigt den Status der TCP/IP-Verbindungen (Ports) zum und vom lokalen Rechner an und kann zur Überwachung von TCP- und UDP-Diensten verwendet werden.

Geben Sie in das Konsolenfenster den Befehl

```
netstat -a
```

ein, zeigt Ihnen XP als Ergebnis eine Liste der geöffneten Ports an. Die vollständige Syntax dieses Befehls erhalten Sie durch die Eingabe von

```
netstat /h
```

Noch ein Hinweis zu netstat: Mit Hilfe des Parameters „Intervall“ legen Sie einen Zeitraum in Sekunden fest, nach der die angezeigten Informationen aktualisiert werden sollen. Ohne die Intervall-Angabe erfolgt die Netstat-Anzeige nur einmal. Sie können das Programm mit der Tastenkombination [Strg]+[C] beenden.

Nslookup: Domain-Namen ermitteln

Mit dem Tool nslookup lässt sich der Domain-Name einer IP-Adresse beziehungsweise die IP-Adresse eines Domain-Namens herausfinden. Standardmäßig – im nicht interaktiven Modus – wird dazu der eingestellte DNS-Server zur Auflösung des Namens oder der IP-Adresse verwendet. Wenn ein anderer DNS-Server zur Auflösung verwendet werden soll, etwa um diesen zu überprüfen, muss mit dem interaktiven Modus eine Verbindung zu diesem Server aufgenommen und mit Befehlen kommuniziert werden. Nslookup steht auf der Kommandozeile als Befehl zu Verfügung.

Geben Sie in der Kommandozeile den Befehl:

```
nslookup <IP-Adresse>
```

oder

```
nslookup <Domänenname>
```

ein. Als Ergebnis gibt das Tool den Domänen-Namen beziehungsweise die IP-Adresse aus.

Nbtstat: Protokollstatistik abrufen

Dieses Programm liefert eine Protokollstatistik und Informationen zu den aktuellen TCP/IP-Verbindungen, die „NetBios over TCP/IP“ verwenden. Es zeigt die Zuordnungen von NetBios-Namen zu IP-Adressen an und benutzt zur Kommunikation die Ports 137, 138 und 139. Die Aufrufsyntax lautet

```
nbtstat /all
```

Die vollständigen Parameter erscheinen nach Eingabe von

```
nbtstat /?
```

auf Ihrem Monitor.

Peter Klau

PROFI-TIPP

Protokolle deinstallieren

Ohne TCP/IP kommen Sie in einem drahtlosen Netzwerk unter Windows XP nicht aus. Dagegen werden IPX/SPX und oft auch Microsoft NetBEUI nicht in jedem Netzwerk benötigt. Überflüssige Protokolle bremsen ein Netzwerk aus. Wenn Sie keine Software installiert haben, die eines dieser Protokolle verwendet, sollten Sie es besser deinstallieren.

1 Öffnen Sie das Fenster „Netzwerkumgebung“ und lassen Sie sich die Netzwerkverbindungen anzeigen.

2 Klicken Sie mit der rechten Maustaste auf die Netzwerkverbindung, wo Sie ein Protokoll entfernen möchten.

3 Wählen Sie im Kontextmenü die Option „Eigenschaften“ aus.

4 Aktivieren Sie anschließend die Registerkarte „Allgemein“.

5 Wählen Sie das Protokoll aus, das Sie entfernen möchten. Klicken Sie dann auf den Button „Deinstallieren“.

6 Danach beenden Sie den Dialog und starten den PC neu. Auf dem gleichen Weg können Sie ein Protokoll auch wieder neu installieren.

WEG DAMIT: Nicht benötigte Protokolle deinstallieren Sie am besten.

PROFI-TIPP

Mehr Tempo via Registry-Tuning

Wer alle Temporeserven aus seinem Netz herausholen möchte, muss an der Windows-Registry schrauben. Ein paar Änderungen in der Registrierdatenbank können nämlich die Systemgeschwindigkeit beträchtlich erhöhen. So lässt sich etwa durch Ausweitung der Paketgröße in stark belasteten Netzwerken das Tempo des Datentransfers optimieren und die Kollisionsgefahr reduzieren. Bei Netzwerken mit eher geringer Belastung, ist eine solche Änderung allerdings meistens nicht notwendig.

1 Starten Sie den Registrierungseditor über „Start | Ausführen“ und „regedit“.

2 Suchen Sie den Eintrag HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters.

3 Dort finden Sie den Parameter TcpWindowSize.

Dieser Wert gibt an, wie viele Bytes empfangen werden können, bevor eine Bestätigung zurückgesendet wird. Standardmäßig liegt dieser Wert bei etwa 8.760 (hängt vom verwendeten Netzwerkadapter ab). Unter XP ist es möglich, diesen Wert auf bis zu 65.535 zu erhöhen. Besitzen Sie ein Windows, das den Parameter TcpWindowSize nicht in der Registry enthält, kann er dort angelegt werden.

Das Ändern dieses Parameters kann signifikante Auswirkungen auf die Leistung des Netzwerks haben. Im allgemeinen gibt es in herkömmlichen Ethernet-Netzwerken – in Abhängigkeit von der Topologie – eine gewisse Latenzzeit zwischen dem Absender und dem Empfänger. Daher sind Kollisionen aufgrund der TCP/IP-typischen Sendung von ACK-Meldungen unwahrscheinlich.

Fehlfunktionen aufdecken

Dem Fehler auf der Spur

Die meiste Zeit funktioniert ein drahtloses Netzwerk völlig einwandfrei. Doch dieser angenehme Zustand währt in der Regel nicht ewig. Besonders nach Änderungen an der Konfiguration ist auch der W-LAN-Alltag nicht mehr so, wie er einmal war. CHIP zeigt Ihnen, was Sie gegen die häufigsten Fehlfunktionen tun können.

Der wichtigste Rat für alle, die unvermutet mit einem streikenden W-LAN konfrontiert werden: Bleiben Sie gelassen und gehen Sie bei der Fehlersuche methodisch vor. Wird ein Notfall-Patient in eine Klinik eingeliefert, raten die Ärzte auch nicht aufs Geratewohl, was ihm wohl fehlen könnte, sondern versuchen, eine exakte Diagnose zu stellen. Anschließend versorgen sie die schlimmsten Verletzungen zuerst und danach kümmern sie sich um die Kleinigkeiten.

Genauso sollten auch Sie bei Problemen im W-LAN vorgehen: Sehen Sie sich die wichtigsten Punkte zuerst an. Probleme im Netzwerk lassen sich nicht im Vorbeigehen lösen und nicht selten müssen Sie eine Menge Zeit investieren. Verschwenden Sie aber keine Zeit, um nach einem Defekt der Netzwerkkarte zu suchen, wenn der Server des Internet-Anbieters nicht erreichbar ist. Ein paar sinnvolle Tests helfen Ihnen bei der W-LAN-Diagnose. Auf diesen Seiten finden Sie die häufigsten Störungen und die besten Lösungsansätze.

Geringe Signalstärke im W-LAN

Besonders in Gebäuden ist die Signalstärke nicht überall gleich gut, denn es gibt immer Räume, die von der Signalstärke her nicht optimal versorgt sind. Mit einigen geeigneten Maßnahmen erhöhen Sie die Signalstärke im gesamten W-LAN. Zur Messung der Signalstärke können Sie Programme wie den Network Stumbler (auf Heft-DVD) verwenden, häufig wird der Wert auch von der Netzkarten-Software angezeigt.

Überprüfen Sie die Signalstärke auf mehreren Computern. Auf diese Weise lässt sich das Empfangsproblem auf einen bestimmten Computer oder Access Point eingrenzen.

Stellen Sie den Access Point, die externe Antenne oder den Computer an einer anderen Stelle im Raum auf. Das genügt oft schon, um den Empfang spürbar zu verbessern.

Platzieren Sie die Antenne oder den Access Point an einem höher gelegenen Standpunkt.

Gibt es einen Mikrowellenherd, Metall, Stromleitungen oder Spiegel in der Nähe des Access Points, wird das Signal oft gestört. Platzieren Sie den Access Point daher an einer anderen, möglichst zentralen Stelle.

Überprüfen Sie die Antennen, insbesondere die externen Antennen, auf korrekten Anschluss. Das gilt für den Access Point und für die Clients.

Auch wenn es nicht immer möglich ist: Versuchen Sie, den Client-Computer näher an den Access Point zu bringen. Das ist die einfachste und preiswerteste Lösung.

Die Antennen der Access Points und W-LAN-Karten sind oft nicht besonders gut. Schließen Sie bei schlechter Signalqualität eine Hochleistungsantenne an den Access Point an. Selbst eine kleine Antenne für den Innenbereich erhöht die Empfangsqualität beträchtlich. Können Sie an den Access Point keine externe Antenne anschließen, versuchen Sie es mit einer besseren Antenne oder einem Signalverstärker.

Stellen Sie zusätzliche Access Points in den Räumen auf und aktivieren Sie das Roaming. Auf diese Weise erweitern Sie die Reichweite des drahtlosen Netzwerks.

Die Verbindung bricht immer wieder ab

Es ist schon merkwürdig: Die meiste Zeit ist der Empfang gut, nur manchmal wird es schwierig und es kommt zu Verbindungsabbrüchen. Die Ursachenforschung ist nicht ganz einfach. Achten Sie auf die folgenden potenziellen Störquellen.

Es befindet sich ein Mikrowellenherd in der Nähe, der ab und zu benutzt wird. Diese Geräte erzeugen Interferenzen auf der 2,4-GHz-Frequenz. Überprüfen Sie das, indem Sie den Herd einschalten und die Signalstärke messen. Häufig lösen Sie das

NACHMESSEN: Gibt es Probleme mit der Signalstärke, messen Sie zunächst mit einem Tool wie Network Stumbler die Signalstärke auf allen Computern im W-LAN.

CHIP → DVD-CODE W-LAN

- **Sniffer** Mit dem Network Stumbler zeigen Sie sämtliche Infos zu Ihrem W-LAN, wie SSID, MAC-Adress, WEP-Verschlüsselung oder die Signalstärke des Hotspots an.
- **Analyse** Das Tool WLAN Expert zeigt Signalstärke, Fehler und Interferenzen im Ihrem Wireless-Netzwerk an. Mit Hilfe des Antennen-Tests optimieren Sie Ihren AP-Standort.

Problem, indem Sie für die Mikrowelle einen anderen Standort suchen. Haben Sie ein Heimnetzwerk, können die Probleme auch von einem Herd in der Nachbarschaft verursacht werden. Auch manche Industriebetriebe verwenden Mikrowellen bei der Produktion von bestimmten Gütern.

Auch beim Einsatz von schnurlosen Telefonen, die ebenfalls im Frequenzbereich 2,4 GHz arbeiten, kann es zu Interferenzen mit dem W-LAN kommen. Im Telefon ist vielleicht nur ein Knacken zu hören, das W-LAN kann jedoch völlig gestört sein. Wenn möglich, sollten Sie schnurlose Telefone mit einem anderen Frequenzbereich verwenden.

Halten Sie Ausschau nach weiteren Geräten, die ebenfalls den 2,4-GHz-Bereich benutzen. In Frage kommen etwa elektrische Garagentore, Kameras oder medizinische Geräte. Eventuell ist es möglich, die Betriebszeiten dieser Geräte einzuschränken.

Kein Empfang des W-LAN-Signals möglich

Dicke Mauern oder Betonwände verhindern häufig den Empfang eines W-LAN-Signals, da helfen oft auch kein Verstärken der Antenne oder zusätzliche Access Points. Ein paar Optionen bleiben Ihnen trotzdem.

Muss es wirklich ein drahtloses Netzwerk sein? Oft ist es einfacher, ein paar Löcher zu bohren und ein Ethernet-Netzwerkkabel zu verlegen.

Wenn Sie auf der einen Seite der Wand ein drahtloses Netz aufgebaut haben, verlegen Sie ein Ethernet-Kabel durch die Wand und stellen auf beiden Seiten einen Access Point auf. Verbinden Sie die beiden Access Points mit dem Kabel und die Wand ist kein Hindernis mehr.

Nicht immer ist es möglich, Löcher durch Wände oder Decken zu bohren. In diesem Fall sollten Sie die Leitungen nutzen, die sowieso in jedem Raum liegen: die Stromkabel. Zahlreiche Hersteller bieten Power-Ethernet-Bridges an, die das Stromnetz zum Datentransport nutzen. Diese Powerline-Verbindungen eignen sich auch für den Datentransport über mehrere Stockwerke. Der große Vorteil: Sie sparen die Kosten für die Verkabelung. Nachteil: Die Technik arbeitet nicht immer störungsfrei und die Übertragungsrate ist nicht besonders hoch.

W-LAN-Verbindung kommt nicht zustande

Die W-LAN-Computer erkennen den Access Point, eine Verbindung zwischen ihnen kommt aber nicht zustande. Häufig liegt das an falschen Sicherheitseinstellungen, aber auch andere Gründe kommen in Betracht.

Überprüfen Sie, ob nur ein bestimmter Client oder alle Geräte keine Verbindung zum Access Point aufbauen können. Dadurch können Sie das Problem oft auf einen bestimmten Client eingrenzen.

Es kann sein, dass die Clients zu weit entfernt vom Access Point positioniert sind, sodass eine zuverlässige Verbindung nicht zustandekommt. Viele signalabhängige Komponenten arbeiten nicht, wenn keine hinreichende Signalstärke vorliegt. Messen Sie die Signalstärke mit einem Tool wie Network Stumbler oder ähnlicher Software. Holen Sie die Clients näher an den Access Point heran; eventuell verschwindet das Problem dann.

Überprüfen Sie, ob die Benutzer den WEP- oder WPA-Key korrekt eingegeben haben. Besonders der bis zu 26 Zeichen lange →

PROFI-TIPPS

W-LAN-Probleme lösen

Monitoring-Tool nutzen Access Points bieten neben der Konfigurations-Software in der Regel auch ein Monitoring-Programm zur Überwachung des W-LANs. Mit dieser Software lassen sich in tabellarischer oder grafischer Form statistische Aussagen über den Zustand des drahtlosen Netzes machen. Das ist vor allem bei der Suche nach Problemen in der Netzwerkkonfiguration sehr hilfreich, aber auch, wenn es darum geht, die Leistung zu optimieren.

XP-Assistenten nutzen Windows bietet gleich zwei Assistenten zur Lösung von Netzwerkproblemen (siehe Abbildung unten). Den ersten Assistenten aktivieren Sie im Fenster „Netzwerkverbindungen“ mit der Option „Netzwerkproblembehandlung“. An dieser Stelle sei auch auf die „Netzwerkdiagnose“ hingewiesen. Dieser Assistent lässt sich mit dem Konsolenbefehl „netsh diag gui“ aufrufen.

Updates installieren Für XP-Netze gilt: Sämtliche Updates und Service Packs installieren.

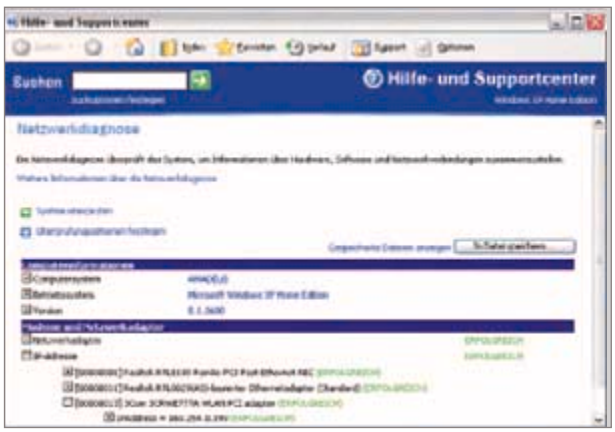
Firmware upgraden Die meisten W-LAN-Netzwerkkarten und Access Points erhalten pro Jahr mehrere Upgrades der Firmware, um Fehler zu beseitigen oder neue Funktionen hinzuzufügen. Es ist deshalb immer eine gute Idee, die Software von der Herstellerseite herunterzuladen und zu installieren.

W-LAN-Karte testen Klicken Sie mit der rechten Maustaste auf das Icon in der Taskleiste. Wählen Sie anschließend die Option „Netzwerkverbindungen anzeigen“. Ist dort kein Netzwerk aufgeführt, empfängt Ihr Netzwerkadapter keine Signale aus dem W-LAN.

Dienste deaktivieren Bieten Access Point und Router des Internet-Providers DHCP- und NAT-Dienste, kommt es zu Konflikten. Deaktivieren Sie diese Dienste auf einem Gerät.

Netzkarten umstecken Bei Netzproblemen hilft es manchmal, die Netzwerkkarten in einen anderen PCI-Slot, PC-Card-Slot oder USB-Port zu stecken. Danach sollten Sie unbedingt einen Neustart vornehmen.

Loopback anpingen Die „Local Loopback Address“ funktioniert wie eine virtuelle Netzwerkkarte. Dafür ist eine spezielle IP-Adresse (127.0.0.1) reserviert, sodass ein Host eine Nachricht an sich selbst schicken kann, beispielsweise zu Testzwecken. Das Anpingen der Loopback-Schnittstelle („ping localhost“ oder „ping 127.0.0.1“) ist eine beliebte Prüfmethode, um zu erfahren, ob der TCP/IP-Stack richtig funktioniert. Das kann völlig ohne Netzwerkanschluss erfolgen und ist sehr hilfreich, um verschiedene Dienste zu prüfen, ohne sie einem entfernten Zugriff zugänglich zu machen.



AUFSCHLUSSREICH: Den Diagnose-Assistenten von Windows XP finden Sie im „Hilfe- und Supportcenter“.

WEP-Schlüssel ist eine häufige Fehlerursache, denn schon ein Fehler kann das ganze System lahmlegen. Es gibt nämlich WEP- oder WPA-Software, die Falscheingaben ohne Fehlermeldung zulässt. Das ist nicht gerade benutzerfreundlich und macht die Fehlersuche häufig recht aufwendig.

Schalten Sie WEP, WPA und MAC-Addressen-Filterung im Access Point vorübergehend ab. Auf diese Weise finden Sie ebenfalls heraus, was die Clients an der Verbindung zum Access Point hindert.

Stellen Sie sicher, dass im Netzwerknamen keine Sonderzeichen oder Leerzeichen vorkommen.

Schalten Sie den Access Point aus, warten Sie 30 Sekunden und schalten Sie danach das Gerät wieder ein. Führen Sie diesen Reset aber nur durch, wenn im Netzwerk gerade keine wichtigen Dinge ablaufen. Bei dieser Aktion verlieren zwangsläufig alle Benutzer den Zugang zum Netzwerk, weil danach vom DHCP-Server meistens neue IP-Adressen vergeben werden. Kleiner Tipp: Manche älteren Gateways oder Access Points müssen regelmäßig neu gebootet werden. Abhilfe schafft an dieser Stelle oft ein Upgrade der Firmware.

Wenn Computer etwa unter Windows XP eine Verbindung zum Netzwerk bekommen, mit einem anderen Betriebssystem aber nicht, kann das der Hinweis auf ein IEEE-802.X-Authentifizierungs-Problem sein. Diese Authentifizierung, als Tool für große Unternehmens-Netzwerke gedacht, wird nur dann unterstützt, wenn sie auf jedem drahtlosen Client installiert ist. Installieren Sie in diesem Fall die IEEE-802.X-Authentifizierung auf allen Computern im Netz oder deaktivieren Sie diese Funktion.

Überprüfen Sie, ob alle Computer den gleichen Netzwerknamen beziehungsweise den gleichen Arbeitsgruppennamen verwenden. Besonders bei Notebooks sind diese Bezeichnungen häufig nicht identisch.

Verwenden Sie in Ihrem drahtlosen Netzwerk Wireless-USB-Adapter, stellen Sie sicher, dass der USB Master Hub korrekt konfiguriert ist.

Keine Verbindung zwischen Ethernet und W-LAN

Manchmal kommt zwischen den Computern im leitungsgebundenen Ethernet und den W-LAN-Rechnern keine Verbindung zustande. In den meisten dieser Fälle ist das auf falsche Einstellungen des Access Points oder auf defekte Kabel zurückzuführen. Überprüfen Sie aber auch die folgenden Möglichkeiten, die für eine solche Verbindungsstörung in Frage kommen können.

Kontrollieren Sie am Access Point, ob er eingeschaltet ist und ob die Verbindung zwischen drahtlosem Netzwerk und Ethernet korrekt konfiguriert ist.

PROFI-TIPPS

Häufige Fehler im W-LAN und ihre Lösung

Fehler/Symptom	Mögliche Lösung
Die LED leuchtet nicht.	Stellen Sie sicher, dass die Karte richtig im Schacht steckt. Überprüfen Sie mit dem Gerätemanager, ob Windows die Karte erkennt.
W-LAN-Karte wird unter Windows als unbekanntes Gerät aufgeführt.	Entfernen Sie die Karte und installieren Sie sie erneut. Stellen Sie sicher, dass der richtige Treiber verwendet wird. Besorgen Sie sich gegebenenfalls den aktuellen Treiber von den Internet-Seiten des Herstellers.
Das Installationsprogramm kann nicht ordnungsgemäß beendet oder der Treiber nicht geladen werden.	Schauen Sie mit dem Windows-Gerätemanager nach, ob ein Hardware-Konflikt vorliegt.
Der Empfang der Datenpakte ist schlecht und wird häufig unterbrochen.	Dies deutet auf ein Antennen-Problem hin. Platzieren Sie die Antenne so, dass keine anderen Geräte (schnurlose Telefone, Mikrowellenherd, elektronische Geräte etc.) den Empfang stören können. Ist das Signal schwach, drehen Sie – wenn möglich – die Antenne. Verwenden Sie eine leistungsstärkere Antenne. Stellen Sie den Computer an einem anderen Ort auf.
Das Betriebssystem erkennt die W-LAN-Karte nicht.	Überprüfen Sie, ob die Karte richtig im Schacht steckt.
Das Netzwerk wird nicht angezeigt.	Starten Sie die Computer neu und warten Sie ein paar Minuten.
Keine Funkverbindung, das Netzwerk funktioniert nicht.	Die Installation war fehlerhaft oder wurde abgebrochen. Installieren Sie die Treiber- und Konfigurations-Software neu. Sind die SSID richtig eingegeben? Ist der Netzwerktyp – Ad-hoc oder Infrastucture – richtig eingestellt? Verwenden Sie die gleiche Schlüssellänge bei der Verschlüsselung?
Die Funkverbindung ist gut, aber die Computer bekommen keine IP-Adressen.	Wenn Sie Windows 2000 oder XP benutzen, sehen Sie nach, ob der DHCP-Client läuft. Sie finden ihn unter „Systemsteuerung | Verwaltung | Dienste | DHCP-Client“.
Die Verbindung bricht ab, die logische Konfiguration geht verloren.	Gelegentlich ist es nötig, alle Geräte aus- und wieder einzuschalten und zwar in der Reihenfolge WAN (Breitband-Modem), Access Point, Workstation.
Der Datendurchsatz im Access Point lässt auf einmal schlagartig nach. Einen Hardware-Fehler können Sie ausschließen.	Ihr Nachbar hat einen Access Point in Betrieb genommen, der auf der gleichen Frequenz arbeitet. Wechseln Sie zu einem anderen Channel.
Der Datendurchsatz im Netzwerk ist schlecht.	Suchen Sie für den Access Point einen neuen Standpunkt. Schon ein paar Zentimeter weiter können bessere Empfangsbedingungen herrschen. Denken Sie daran, dass die 54 MBit/s von 802.11g nur ein theoretischer Wert sind. Wenn Sie 38 MBit/s erreichen, dürfen Sie sich freuen.

Falls Sie einen Software-Access-Point verwenden, überprüfen Sie am besten, ob die Einstellungen noch korrekt sind und nicht etwa durch einen Bootvorgang oder eine andere Manipulation verändert wurden.

Überprüfen Sie, ob die Kabel richtig eingesteckt sind. Auch ein beschädigtes Kabel kann für die Verbindungsstörung zwischen Ethernet und W-LAN verantwortlich sein.

Haben Sie ein Netzwerk mit mehreren drahtgebundenen Computern aufgebaut, schauen Sie nach, ob auch eine Verbindung zwischen diesen besteht.

Schalten Sie das Wireless Gateway aus und starten Sie das Gerät nach kurzer Zeit neu.

Ziehen Sie das Kabel aus dem Gateway, warten Sie 30 Sekunden und stecken Sie das Kabel wieder ein. Manchmal reicht das schon, um einen Fehler zu beseitigen.

Besteht das Problem bei einem speziellen Dienst, beispielsweise beim Printer Sharing, stellen Sie sicher, dass die entsprechende Software auf allen beteiligten Computern auch installiert und richtig konfiguriert wurde.

Internet-Verbindung kommt nicht zustande

Das drahtlose Netzwerk funktioniert tadellos, aber eine Internet-Verbindung über ein analoges Modem, DSL-Modem oder Breitbandkabel kommt nicht zustande. Dafür können eine Menge Faktoren verantwortlich sein. Gehen Sie einmal die folgenden möglichen Störungsursachen durch.

Verwenden Sie die dynamische Adressierung, sollten Sie überprüfen, ob jeder Computer im Netzwerk eine DHCP-Adresse erhält. Falls das nicht der Fall ist, haben Sie ein Problem mit dem Gateway oder dem DHCP-Server.

Befindet sich der DHCP-Server in einem Access Point, kann es sein, dass nicht alle Computer mit Adressen versorgt werden. Die meisten DHCP-Server müssen dafür speziell konfiguriert werden, wenn sie auch für die drahtgebundenen Netzwerk-Computer IP-Adressen bereitstellen sollen.

Auch das kommt vor: Jemand hat ein Ad-hoc-Netzwerk mit demselben Namen eingerichtet, den Sie benutzen. Sie umgehen das Problem, indem Sie bestimmte Namen für Infrastruktur-Netzwerke reservieren.

Überprüfen Sie die Firewall-Einstellungen: Um mit Access Points zusammenzuarbeiten, empfangen Computer oder andere Geräte DHCP-Broadcast. Eine „übersensibel" eingestellte Firewall kann unter Umständen den DHCP-Broadcast unterdrücken, auch wenn er aus dem lokalen Netzwerk kommt.

Wenn im Netzwerk gerade keine wichtigen Dinge stattfinden, schalten Sie den Access Point aus und wieder ein (oder drücken →

Sie den Reset-Knopf). Manchmal hilft es auch, das Kabel abzuziehen und nach etwa 30 Sekunden wieder anzuschließen.

Überprüfen Sie, ob alle Kabel für die Internet-Verbindung (zum Modem oder Router) unbeschädigt und korrekt eingesteckt sind.

Führen Sie ein Reset am analogen Modem, DSL-Modem oder Kabelmodem durch oder entfernen Sie die entsprechenden Kabel für etwa 30 Sekunden.

Wenn die Aktivitäten im Netzwerk es zulassen, führen Sie erneut ein Reset am Modem oder Router durch, schalten Sie jedoch vorher das Gateway aus. Schalten Sie das Gateway erst wieder ein, nachdem das Modem hochgefahren ist.

Falls es möglich ist, verbinden Sie einen Computer direkt mit dem Modem oder Router. Bekommen Sie weiterhin keine Verbindung zum Internet, ist es an der Zeit, die Hotline Ihres Internet-Providers zu kontaktieren.

Schreiben Sie sich die Werte Ihrer Einstellungen für das drahtlose Gateway auf und setzen Sie das Gerät auf die Werkseinstellungen zurück. Geben Sie danach erneut Ihre Werte ein.

Aktualisieren Sie die Firmware für Ihren Access Point.

Versuchen Sie, eine Internet-Verbindung über verschiedene Gateways oder Access Points herzustellen.

WDS funktioniert nicht

Sie haben ein Wireless Distribution System (WDS) im Einsatz und versuchen, verschiedene Access Points zu verbinden – ohne Erfolg. Verwenden Sie Geräte verschiedener Hersteller, haben Sie schlechte Karten. Ein korrekt funktionierendes Wireless Distribution System erfordert dann ein gründliches Studium der Handbücher und die manuelle Eingabe zahlreicher Parameter. Aber auch die folgenden Fakten sollten Sie bei einem streikenden Wireless Distribution System beachten.

Überprüfen Sie, ob Sie alle MAC-Adressen korrekt eingegeben haben. MAC-Adressen bestehen aus sechs Gruppen zu je zwei Zeichen. Ein Fehler reicht, damit die Verbindung scheitert.

Kontrollieren Sie, ob jeder Access Point im Wireless Distribution System mit dem Master-Access-Point kommunizieren kann. Verändern Sie gegebenenfalls die Standorte der Access Points, bis die Signalstärke ausreicht.

Verwenden Sie Access Points von unterschiedlichen Herstellern, führen Sie ein Upgrade der Firmware durch.

Ping-Test vornehmen

Eine der einfachsten Möglichkeiten, eine Verbindung zu überprüfen, ist der Ping-Test. Wie eine Art Sonar sendet das Tool ein Datenpaket zu einem anderen Netzwerkgerät und wartet auf das Echo. Kommt eine Antwort, sind beide Computer verbunden. Zum Durchführen des Ping-Tests benötigen Sie die IP-Adresse oder den Namen des Ziel-Computers.

Zum Feststellen der aktuellen IP-Adresse können Sie den Befehl „ipconfig“ (siehe Abbildung unten) verwenden. Unter Windows XP erhalten Sie diese Angaben auch, wenn Sie rechts auf das Verbindungs-Icon in der Taskleiste klicken und im Kontextmenü die Option „Status“ wählen. Die IP-Adresse finden Sie auf der Registerkarte „Details“.

Nachdem Sie die IP-Adresse ermittelt haben, geben Sie am DOS-Prompt oder im Fenster „Ausführen“ den Befehl

```
ping <IP-Adresse>
```

oder

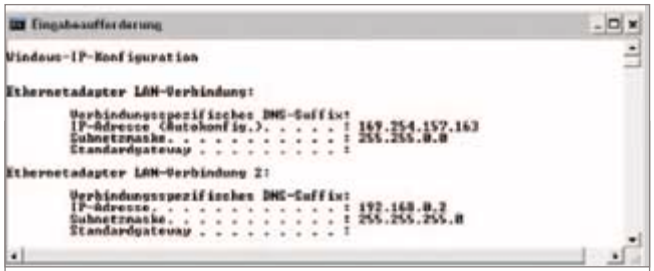
```
ping <Rechnername>
```

ein. Der Ping-Test ist erfolgreich, wenn als Ergebnis neben anderen Angaben eine Liste der gesendeten, empfangenen und verlorenen Pakete vorliegt. Die Meldung „Destination host unreacheable“ besagt, dass keine Route zum Zielcomputer gefunden werden konnte, was wiederum auf ein Verbindungsproblem hindeutet. Überprüfen Sie, ob der Local Host und das Gateway korrekt konfiguriert sind.

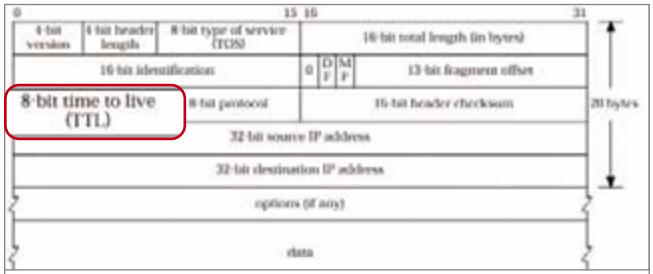
Gibt Ping die Meldung „Requested time out“ aus, hat der Zielcomputer die Anfrage innerhalb eines bestimmten Zeitraums (festgelegt durch den Parameter „-t“) nicht empfangen. Das ist ein typischer Hinweis darauf, dass der Zielcomputer nicht im Netzwerk ist. Entweder ist er ausgeschaltet oder nicht richtig konfiguriert. Es kann auch bedeuten, dass ein Netzwerkgerät nicht richtig funktioniert. In seltenen Fällen bedeutet die „Time out“-Meldung, das im Netzwerk so viel Traffic ist, dass der Zielcomputer nicht erreicht werden konnte oder dass die falsche IP-Adresse verwendet wurde. In all diesen Fällen sollten Sie versuchen, mit Hilfe anderer Tools, manueller Inspektion und Überprüfung der Clients- und Gateway-Konfiguration eine sorgfältige Diagnose zu stellen.

Kann der Hostname nicht aufgelöst werden, gibt Ping die Meldung „Unknown host“ heraus. Dieser Fehler tritt meist bei der falschen Eingabe des Hostnamens auf oder wenn der DNS-Dienst oder WINS-Server nicht richtig konfiguriert oder erreichbar ist. An dieser Stelle kann der Befehl „nslookup“ (siehe auch 127) weitere Klärung bringen.

Durch das Feld „Time to Live“ (TTL) im IP-Header ist für jedes IP-Paket eine maximale Lebensdauer festgelegt. Unter Windows können Sie mit dem Parameter „-i“ die Lebensdauer des Pakets beeinflussen. Die relative Lebensdauer eines Pakets


Eingabeaufforderung
Windows-IP-Konfiguration
Ethernetadapter LAN-Verbindung:
Verbindungsspezifisches DNS-Suffix:
IP-Adresse (Autokonfig.) . . . . : 169.254.157.163
Subnetzmaske . . . . . : 255.255.0.0
Standardgateway . . . . . :
Ethernetadapter LAN-Verbindung 2:
Verbindungsspezifisches DNS-Suffix:
IP-Adresse . . . . . : 192.168.0.2
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . :

AUSKUNFTSFREUDIG: Nach der Eingabe von „ipconfig“ informiert Sie das Tool über Einzelheiten der IP-Konfiguration wie IP-Adresse, Subnetzmaske und Standard-Gateway.



LEBENSDAUER: Im Feld „Time to Live“ (TTL) im IP-Header ist für jedes IP-Paket die maximale Lebensdauer festgelegt. Sie lässt sich mit dem Parameter „-i“ modifizieren.

beträgt maximal 255 Sekunden oder das Durchlaufen von 255 Routern. Erhalten Sie die Fehlermeldung „TTL expired in transit“, haben Sie mit hoher Wahrscheinlichkeit ein Routing-Problem in Ihrem Netzwerk.

Netzverbindung testen und erneuern

Zur Ermittlung der IP-Adresse öffnen Sie das Fenster „Eingabeaufforderung“ und geben den Befehl

```
ipconfig
```

ein. Als Ergebnis erhalten Sie die Angaben, die Sie in der Abbildung unten links sehen.

Falls Sie keine IP-Adresse sehen, befindet sich Ihr Rechner nicht im Netzwerk. Um eine automatisch zugeteilte Adresse zu erneuern, geben Sie

```
ipconfig /renew
```

oder

```
ipconfig /release
```

ein. Der Parameter „renew“ erneuert die IP-Adressen für alle Netzwerkadapter. Verwenden Sie den Parameter „release“, gibt XP die IP-Adresse für den aktuellen Netzwerkadapter frei. Lesen Sie die Meldung, dass keine IP-Adresse zugeordnet werden konnte, haben Sie ein Problem mit dem Dynamic Host Configuration Protocol (DHCP).

Zum Testen der IP-Verbindung können Sie auch den Befehl „net view“ (siehe auch 126) verwenden. Für Windows XP mit Service Pack 2 liefert der Befehl „netstat -banvo“ ein ausführliches Protokoll aller aktiven Netzverbindungen mit verwendetem Protokoll, lokalen und remote IP-Adressen, der zuständigen ausführbaren Datei und allen aufgerufenen Komponenten.

Peter Klau

KNOW-HOW

So finden Sie alle Fehler – im Ethernet und im W-LAN

Doktern Sie nicht an Symptomen herum, sondern versuchen Sie herauszufinden, was den oder die Fehler verursacht hat. Wenn Sie ohne Konzept an die Sache herangehen, komplizieren Sie die Situation eventuell. Die beste Methode besteht darin, alles aufzuschreiben: die Ereignisse, Symptome und besonders die Fehlermeldungen. Mit den folgenden fünf Schritten gehen Sie allen Netzwerk-Problemen wirklich auf den Grund.

1. Problem beschreiben Identifizieren Sie zunächst das Problem und sammeln Sie alle Informationen darüber. Das ist recht einfach, denn die meisten Probleme sind nicht schwer zu finden. Vielleicht können Sie keine E-Mail senden oder ein Computer ist im Netzwerk nicht sichtbar.

Ist das Problem reproduzierbar oder tritt es periodisch auf? Periodisch auftretende Probleme sind meistens schwieriger zu verfolgen, weil sie von bestimmten Variablen, Zuständen oder Zeiten abhängig sind. Reproduzierbare Probleme müssen in der Regel sofort gelöst werden, weil sonst kein weiteres Arbeiten möglich ist.

Richten Sie Ihre Aufmerksamkeit auf alle sichtbaren Indikatoren. Fast alle Netzwerkkarten verfügen über LEDs, die Betriebszustand und Datenfluss anzeigen. Ist diese Anzeige außer Betrieb oder wird ein fehlerhafter Betriebszustand angezeigt, sollten Sie diese Information Ihrer Fehlerbeschreibung hinzufügen.

Notieren Sie alle Fehlermeldungen oder das Fehlen einer solchen Meldung. Schreiben Sie die genauen Symptome auf oder machen Sie einen Screenshot. Jeder Buchstabe oder jede Fehlernummer kann wichtig sein.

2. System auseinandernehmen Um einen Fehler zu finden, ist es oft erforderlich, Teile des Netzwerks zu separieren, um den Fehler einzugrenzen. Danach können Sie die einzelnen Komponenten analysieren. Das Schwierige besteht darin, herauszufinden, wie man ein System am sinnvollsten unterteilt und in welchem Segment der Fehler aufgetreten ist. Manchmal ist es möglich, ein Segment noch weiter zu unterteilen oder die Fehlersuche auf einen Rechner, etwa einen File-Server, zu konzentrieren.

Schreiben Sie alle Variablen auf Ihren Zettel und zeichnen Sie gegebenenfalls ein Diagramm, auf dem erkennbar ist, wie das System zusammenhängt. Ein Diagramm ist besonders hilfreich, wenn Kabel im Spiel sind und Sie diese nach der Reparatur wieder anschließen müssen.

3. Die richtigen Fragen stellen Nachdem Sie die einzelnen Teile des Systems identifiziert haben, können Sie vorsichtig daran gehen, jedes Teil des Netzwerks auf sein Potenzial als Fehlerquelle zu untersuchen.

Dazu sollten Sie sich einen Katalog mit Fragen zusammenstellen, beispielsweise: Haben Sie irgendetwas geändert? Wurde das System neu gestartet (immer einen Versuch wert)? Bei welchen Computern tritt der Fehler auf? Besteht eine Verbindung zum Access Point? Tritt das Problem zu einem bestimmten Zeitpunkt auf? Ist das Problem reproduzierbar?

Schreiben Sie die Fragen auf und nummerieren Sie sie. So können Sie sich leicht an sie erinnern, wenn Sie versuchen durch Tests die Antworten zu finden.

4. Antworten finden Nachdem Sie den Fragenkatalog zusammengestellt haben, überlegen Sie sich, welche Schritte notwendig sind, um die Fragen zu beantworten. Unterteilen Sie die Fragen in: „leicht zu beantworten“, „schwer zu beantworten“ und „sehr schwer zu beantworten“.

Beginnen Sie zunächst, Antworten für die leichten Fragen zu finden. So werden Sie etwa leicht ein herausgezogenes Ethernet-Kabel finden oder eine nicht funktionierende LED. Arbeiten Sie die Fragen Schritt für Schritt ab. Schreiben Sie auf, was beim Testen passiert. Wenn Sie etwas ändern, schreiben Sie das ebenfalls auf, sodass Sie die Geräte später wieder in den ursprünglichen Zustand versetzen können.

5. Hilfe holen In den meisten Fällen finden Sie bei der schrittweisen Beantwortung der Fragen das Problem und seine Lösung. Aber was ist, wenn Sie den Fehler nicht finden oder ihn zwar lokalisieren, aber nicht beseitigen können? An dieser Stelle kommen die Experten ins Spiel. Ein Experte ist jemand, der schon alle Fehler gemacht hat und Schritte zu ihrer Korrektur kennt. Doch an wen sollen Sie sich wenden, wenn Sie keinen dieser Experten kennen?

Lösung 1: Gönnen Sie sich zehn Minuten und fragen Sie Google oder eine andere Suchmaschine. Das ist am schnellsten, einfachsten und preiswertesten.

Lösung 2: Fragen Sie in den entsprechenden Newsgroups, Foren oder Mailing-Listen nach den Antworten.

Lösung 3: Werden Sie im Internet nicht fündig, wenden Sie sich an den Support der Hardware-Hersteller. Zwar sind die Hotlines häufig überlastet und es gibt auch keine Garantie, dass man Ihnen dort helfen kann. Doch weil sich die Mitarbeiter der technischen Hotline mit den eigenen Produkten in der Regel gut auskennen, stehen die Chancen auf Hilfe dort recht gut. Sie erhöhen diese Chancen, wenn Sie die folgenden Angaben machen können:

- **Computer-Modell(e)**, Größe des Arbeitsspeichers, Version des Betriebssystems
- **Jede Änderung** am System, Upgrade des Betriebsystems, neu installierte Treiber
- **Spezielle Erweiterungen**, Addons, Firewalls etc.
- **Verwendete Netzwerk-Hardware**, Access Points, W-LAN-Karten, Antennen etc. sowie die Versionen der Treiber

W-LAN-Tipps für Profis

Perfekt funken im W-LAN

Einfache Oberflächen, Assistenten, automatische Konfiguration – meist ist das ein Wunschtraum bei W-LANs. CHIP zeigt, wie Sie Ihr W-LAN trotzdem perfekt einrichten können und dabei nicht nur mehr Leistung bekommen, sondern Ihr Netzwerk auch noch vor fremden Zugriffen von Hackern schützen können.

Schön, wenn es einmal läuft, das drahtlose Netzwerk – doch bis dahin ist es meist ein weiter Weg. Bei den Herstellern der Netzwerkkomponenten melden sich jeden Tag mehrere hundert Anrufer, die Probleme beim Einrichten des W-LANs haben. Und wenn es erst einmal läuft, sind viele User so glücklich, dass sie vergessen, das Netzwerk gegen Eindringlinge abzusichern. So schätzen Experten der Universität Rostock, dass jedes vierte W-LAN ohne WEP oder WPA Codierung seine Daten in die Welt hinausfunkt.

Aber das ist noch nicht alles. Die Hindernisse auf dem Weg zum perfekten Funknetz sind zahlreich: So scheitert das kabellose Surfvergnügen an der geringen Reichweite oder an der Inkompatibilität der einzelnen Geräte, die nicht hundertprozentig nach den 802.11-Standards des IEEE-Konsortiums (Institute of Electrical and Electronics Engineers) arbeiten. Aber verzweifeln muss man deshalb trotzdem nicht, den für die meisten Probleme gibt es auch eine Lösung.

CHIP hat sich der Sache einmal angenommen und zeigt nicht nur, was Sie machen müssen, wenn sich Access Point (AP) und Netzwerkadapter mal nicht verbinden wollen, sondern gibt zusätzlich noch Infos zu aktuellen Verschlüsselungsmethoden und zeigt, was die Zukunft zu bieten hat.

Aber damit nicht genug. In diesem Artikel erfahren Sie, wie Sie spezielle Firmware auf den Router aufspielen können und damit nicht nur die Reichweite immens erhöhen, sondern auch geheime Features der Geräte freischalten können, die normalerweise nur den Herstellern der Komponenten vorbehalten sind.

Geheime Firmware aufspielen

Hersteller bieten mit neuen Firmware-Versionen nicht nur Bugfixes an, sondern erweitern in manchen Fällen die Geräte sogar um zusätzliche Features. So lassen sich beispielsweise viele Access Points mit Hilfe der Software-Upgrades auf den Verschlüsselungsstandard WPA (Wi-Fi Protected Access) aufrüsten. Ob das auch bei Ihrem AP funktioniert, erfahren Sie auf der Webseite des Herstellers.

CHIP → DVD-CODE W-LAN

- **W-LAN optimieren** Auf Heft-DVD finden Sie das Profi-Tool Airopeek SE als Demo, mit dem Sie umfangreiche Site Surveys vornehmen. Alternative: Das Gratis-Tool NetStumbler.
- **Analyse-Tool** Die Gratis-Software WLAN Expert zeigt Signalstärke, Fehler und Interferenzen von WLAN-Netzen an. Zusätzlich ist ein grafischer Antennentest integriert.

Doch damit nicht genug: findige Programmierer haben sich das eingebaute Betriebssystem bekannter APs angeschaut und ihre eigenen Versionen entwickelt. Diese lassen sich statt des Originals aufspielen und bieten bei manchen Geräten erstaunliche Zusatzfeatures, wie etwa eine weit erhöhte Reichweite oder die Möglichkeit, eigene W-LAN-Kanäle zu definieren. Allerdings hat die Sache einen Haken: Die neue Software ist nicht von den Herstellern autorisiert und wird daher von den Support-Hotlines nicht unterstützt. Trotzdem, einen Versuch ist es auf alle Fälle wert. Im schlimmsten Fall spielen Sie die alte Firmware einfach wieder auf – damit ist der AP dann wieder voll funktionsfähig. Die neue Firmware spielen Sie genauso auf, als ob Sie eine Original-Version auf dem Access Point updaten würden.

Die neuen Firmware-Versionen liegen auf speziellen Seiten im Internet; im Kasten auf 135 finden Sie die besten Internet-Links, über die Sie an die speziellen Betriebssystem-Versionen gelangen können.

Reichweite mit 802.11b erhöhen

Grundsätzlich gilt: Umso weiter die Entfernung zwischen Access Point und PC-Adapter, desto geringer die Geschwindigkeit. In der Praxis schalten deshalb die meisten Access Point ganz automatisch die Übertragungsrate herunter, wenn sich der Computer zu weit entfernt, und versuchen so, die Verbindung zu halten. Manche Hersteller liefern allerdings ihre Geräte so konfiguriert aus, dass diese nicht selbstständig die Geschwindigkeit herunterschalten und damit die Reichweite stark einschränken. Besonders bei reinen Internet-PCs steht aber eine große Netzabdeckung im Vordergrund. DSL ist mit durchschnittlich 2 bis 3 MByte/s relativ langsam; setzen Sie daher bei Ihrem AP den Übertragungsstandard auf 802.11b fest. Dieser ist mit rund 8 MByte/s vollkommen ausreichend für den Internetzugang. Der Vorteil: Mit dem langsameren Standard erhöhen Sie die Reichweite Ihres Drahtlosnetzwerkes um bis zu 40 Prozent.

Wir erklären am Beispiel eines Vigor 2900 von DrayTek wie Sie vorgehen müssen, bei allen anderen Modellen ist die Vorgehensweise analog. Klicken Sie im Hauptmenü auf „Wireless LAN Setup“ und dort auf „General Settings“. Unter „Mode“ markieren Sie „11b only“ und bestätigen mit „OK“. Im Hauptmenü starten Sie mit „Reboot System“ den Access Point neu.

Apple und Windows verbinden

Zwar gibt es einen gemeinsamen W-LAN-Standard, nämlich IEEE802.11g, trotzdem kommt es immer wieder zu Problemen bei gemischten Netzwerken mit Windows und Apple Rechnern. Meist ist daran die Verschlüsselung schuld. Versuchen Sie des-

Die besten W-LAN-Seiten im Web

Die Infoseite für Linksys → www.linksysinfo.org/index.php
Hier erfahren Sie die akuellen Firmware-Versionen.
Technische Details zu Firmware & Co → www.seattlewireless.net/index.cgi/WAP54G
Wer sich genauer mit Firmware-Updates beschätigen will, ist hier gut aufgehoben – viele Infos und Tipps.
Gepachte Firmware → www.vallstedt-networks.de
Hier finden Sie unter anderem angepasste Firmware-Versionen.

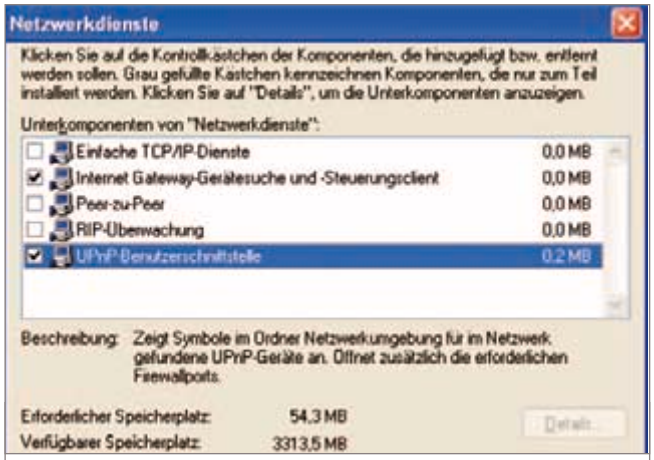
halb vorrübergehend die WEP und WPA Codierung bei Ihrem Access Point abzuschalten, um anschließend den Windows-PC und den Apple-Rechner darüber zu verbinden.

Hilft das nichts, verwenden Sie bei der WEP-Verschlüsselung nur hexadezimale Zeichen und nicht alphanumerische. Windows versteht beide Systeme, bei Apple gibt es Ausnahmen. Für eine 64 Bit WEP-Codierung brauchen Sie zehn HEX-Zeichen, bei 128 Bit sind es 26. Die numerischen Zeichen müssen zwischen 0 und 9 liegen, die Buchstaben zwischen A und F. Eine 64-Bit-Verschlüsselung könnte also wie folgt aussehen: „123F56E890“. Wer will, kann das Tool auf der Homepage **http://home.arcor.de/gybrsh2/pw/wep.html** verwenden, um sich einen solchen Key errechnen zu lassen.

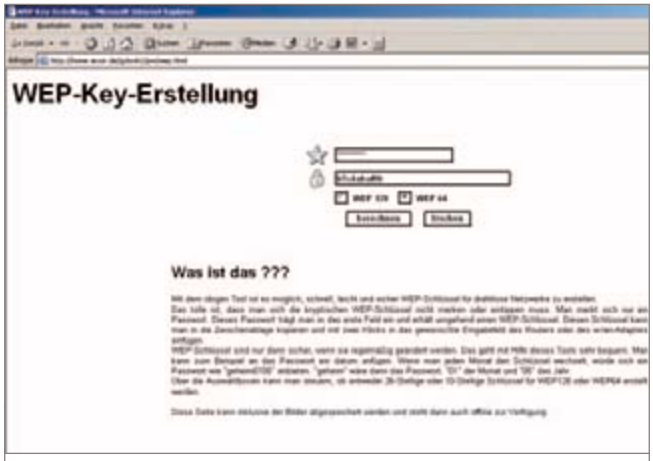
Läuft das Netz immer noch nicht, ist der Access Point nicht hundertprozentig zu beiden kompatibel. Probieren Sie es in diesem Fall mit einem Firmware-Upgrade des APs und der einzelnen Adapter; die notwendige Software finden Sie auf den Herstellerseiten im Internet.

Alte Treiber entfernen

Bei W-LAN-Adaptern kann es vorkommen, dass Sie die Meldung „Bei dieser Geräteinstallation trat ein Fehler auf. Der Name wird bereits als ein Dienstname oder ein Dienstanzeigename verwendet.“ bekommen und der PC die Installation abbricht. Dies liegt nicht am Hersteller der Treiber, sondern an einem Fehler in Windows XP. Die Lösung: Entfernen Sie den alten Treiber, um anschließend die aktuelle Version aufzuspielen.


Netzwerkdienste
Klicken Sie auf die Kontrollkästchen der Komponenten, die hinzugefügt bzw. entfernt werden sollen. Grau gefüllte Kästchen kennzeichnen Komponenten, die nur zum Teil installiert werden. Klicken Sie auf "Details", um die Unterkomponenten anzuzeigen.
Unterkomponenten von "Netzwerkdienste":
Einfache TCP/IP-Dienste 0,0 MB
Internet Gateway-Geräteсuche und -Steuerungsclient 0,0 MB
Peer-zu-Peer 0,0 MB
RIP-Überwachung 0,0 MB
UPnP-Benutzerschnittstelle 0,2 MB
Beschreibung: Zeigt Symbole im Ordner Netzwerkumgebung für im Netzwerk gefundene UPnP-Geräte an. Öffnet zusätzlich die erforderlichen Firewallports.
Erforderlicher Speicherplatz: 54,3 MB
Verfügbarer Speicherplatz: 3313,5 MB
Details...

ROUTER-ZUGRIFF ÜBER WINDOWS: Wenn Sie Ihren Router nicht in den Netzwerkeinstellungen von Windows sehen, müssen Sie den UPnP-Dienst separat nachinstallieren.



EINFACHE KENNWORTVERGABE IM INTERNET: Über die Webseite http://home.arcor.de/gybrsh2/pw/wep.html können Sie sich ganz komfortabel einen WEP-Key errechnen lassen.

Klicken Sie dazu auf „Start“ und dort mit der rechten Maustaste auf „Arbeitsplatz“. Aus dem Kontextmenü wählen Sie „Eigenschaften“ aus und drücken im Reiter „Hardware“ auf „Geräte-Manager“. Erweitern Sie die Rubrik „Netzwerkadapter“, klicken Sie dann mit der rechten Maustaste auf die erste Netzwerkkarte und wählen Sie „Deinstallieren“ aus; bestätigen Sie die Meldung mit „OK“. Verfahren Sie nun so mit allen anderen Netzwerkadaptern im Gerätemanager.

Klicken Sie auf „Start | Ausführen“ und geben Sie „msconfig“ ein. Mit „OK“ starten Sie das Konfigurationstool von Microsoft. Markieren Sie dort den Punkt „Diagnosesystemstart | Nur grundlegende Dienste und Geräte starten“. Im Reiter „Dienste“ setzen Sie noch einen Haken vor „Alle Microsoft-Dienste ausblenden“ und deaktivieren anschließend alle Dienste im obigen Fenster. Bestätigen Sie dann die neuen Einstellungen mit einem Klick auf „OK“ und starten Sie den Rechner neu. Damit stellen Sie sicher, dass kein Dienst die Treiber gerade benutzt und damit die Deinstallation verhindert.

Gehen Sie anschließend in die Registry, indem Sie im Menü „Start | Ausführen“ den Befehl „regedit“ eingeben und auf „OK“ drücken. Im Schlüssel „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services“ suchen Sie nun nach für Ihren Netzwerkadapter bestimmten Registrierungseinträgen, beispielsweise Linksys oder Netgear. Wenn Sie einen Eintrag gefunden haben, löschen Sie ihn. Öffnen Sie wieder das MS-Konfigurationstool mit „Start | Ausführen | msconfig“ und klicken dort auf „Normaler Systemstart | Alle Geräte und Dienste laden“.

Starten Sie den Rechner anschließend neu. Anschließend richtet Windows automatisch die notwendigen Treiber wieder ein – nun können Sie auch den neuen Treiber für Ihre Netzwerkkarte installieren. Als letztes gehen Sie nochmals in das MSConfig-Tool und aktivieren im Reiter „Dienste“ wieder die zuvor deaktivierten Einträge.

Messenger-Probleme lösen

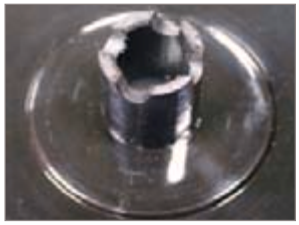
Der MS Messenger ist nicht nur zum Chatten da, er ist gleichzeitig ein kleines Videotelefon. Per Webcam lassen sich so Fotos und Videokonferenzen rund um den Globus schicken, es sei →

PROFI-TIPP

W-LAN-Antenne selber bauen

Externe W-LAN-Antennen sind teuer und passen nicht immer an Ihren Access Point. Am besten bauen Sie sich Ihre eigene – die Experten von Vallstedt-Networks (www.vallstedt-networks.de) zeigen, was Sie brauchen, um die Leistung Ihres W-LANs um bis zu 40 Prozent zu erhöhen. Alles, was Sie benötigen, ist ein bisschen Geschick, Werkzeug und eine ruhige Hand, denn wichtig ist vor allem exaktes Arbeiten.

Das brauchen Sie
CD-Spindel, Lötkolben
Rundfeile (www.conrad.de, 20 Euro)
25cm NYM-Kupferkabel 2,5mm²
Flachrundzange (www.conrad.de, 20 Euro)
SMA-Stecker (www.steckerprofi .com, 5 Euro)
Schieblehre (www.conrad.de, 2 Euro)
RG58-Kabel (www.conrad.de, 2 Euro)



1 | CD-Spindel vorbereiten Kürzen Sie als erstes den CD-Halter der Spindel auf 18 Millimeter. Feilen Sie dann mit einer Rundfeile kleine Schlitze in die Halterung; die Unterkante der Schlitze sollte 16 Millimeter vom Boden entfernt sein.

2 | Antenne biegen Nehmen Sie nun den Kupferdraht und biegen Sie ihn nach 29 Millimetern um 90 Grad. Nach weiteren 29 Millimeter kommt die nächste Biegung, bis das Gerüst letzendlich so aussieht, wie auf dem Foto links.

3 | Kabel anschließen Nun verbinden Sie die offenen Kabelstellen, wie es auf dem Foto zu sehen ist und löten anschließend das Antennenkabel an die beiden Lötstellen. Wenn Sie wollen, können Sie nun bei Bedarf noch einen Schutzlack auftragen.

4 | Antenne anbringen Kleben Sie nun eine CD an den Boden der Spindel und anschließend die Antenne an die Halterung fest. Achten Sie dabei darauf, dass alle Teile der Antenne 16 Millimeter vom Boden entfernt sind. Korrigieren Sie notfalls die Schlitze nach.

5 | Stecker anlöten Als letztes verkleben Sie noch das Kabel am unteren Teil der Spindel für die Zugentlastung. Am anderen Ende des Kabels löten Sie den SMA-Stecker für die Verbindung zum AP an. Jetzt setzen Sie noch die Spindel-Hülle auf – fertig. Die fertige Antenne können Sie nun ganz einfach an Ihren AP anschrauben.

denn der Router macht einen Strich durch die Rechnung. Denn bei bestimmten Routern, die mit UPnP (Universal Plug&Play) arbeiten, kann es zu Problemen kommen. Bis zuletzt ist von Microsoft noch kein entsprechender Patch veröffentlicht worden, der das Problem behebt. Auch Nachfragen bei der Hotline des Software-Riesen brachten keinen Erfolg.

Einen Patch gibt es nicht, eine Lösung allerdings schon. Und so gehen Sie vor: Klicken Sie zunächst im Menü „Start | Systemsteuerung“ auf „Software“ und wählen Sie dort den Punkt „Windows-Komponenten hinzufügen/entfernen“ aus. Markieren Sie anschließend den Punkt „Netzwerkdienste“, drücken Sie auf „Details“ und setzen Sie einen Haken vor „UPnP-Benutzerschnittstelle“. Bestätigen Sie die Einstellungen mit „OK | Weiter“. Stellen Sie anschließend sicher, dass in der Konfiguration Ihres Routers UPnP aktiviert ist.

Öffnen Sie jetzt „Start | Ausführen“ und geben Sie den Befehl „ncpa.cpl“ ein, um die Netzwerkverbindungen aufzurufen. Bestätigen Sie mit „OK“ und klicken Sie im folgenden Fenster mit der rechten Maustaste auf „PPPoE Broadband Connection auf Router“; über „Eigenschaften“ gelangen Sie auf die Einstellungsseite. Drücken Sie dort auf „Einstellungen“ und entfernen Sie alle Häkchen vor den einzelnen Diensten. Bestätigen Sie die Änderungen zweimal mit „OK“ – nun können Sie auch Videokonferenzen über Ihren Router nutzen.

Verbindungsprobleme lösen

Der Access Point ist perfekt eingerichtet, die Funkverbindung ist aufgebaut, das Signal hat fast 100 Prozent – trotzdem funktioniert die Internetverbindung nicht. Das kann mehrere Ursachen habe: Prüfen Sie zunächst, ob Sie eine IP vom Access Point erhalten haben. Klicken Sie dazu im Menü „Start“ auf „Ausführen“ und geben Sie dort „cmd“ ein. In Kommandozeile tippen Sie den Befehl

```
ipconfig /all
```

ein und drücken [Enter]. Unter „IP-Adresse“ sollte eine Zahl mit den Anfangsziffern „192.168“ stehen. Ist das nicht der Fall, prüfen Sie, ob Ihr Router auf den „DHCP“-Modus eingestellt ist.

Bekommen Sie eine IP über den Router zugeteilt, checken Sie ob unter „DNS-Server“ die IP des Access Points steht. Ist das nicht der Fall, geben Sie den Befehl

```
ipconfig /release
```

ein; drücken Sie die [Enter]-Taste und starten Sie den Rechner anschließend neu.

Funktioniert der Internet-Zugang per Wireless LAN immer noch nicht, liegt es eventuell an den Übertragungseinstellungen des Access Points. Um diese Einstellungen richtig zu konfigurieren, beschreiben wir anhand eines Linksys-Routers die Vorgehensweise. Bei Modellen anderer Hersteller ist der Weg prinzipiell derselbe.

Klicken Sie im Hauptmenü der Router-Konfiguration auf den Punkt „Wireless“ und dort auf „Advanced Wireless Settings“. Geben Sie nun unter „RTS Threshold“ den Wert „2304“ ein, unter „Fragmentation Threshold“ den Wert „2304“ und bei „Beacon Interval“ den Wert „50“. Diese Einstellungen ändern die Paketgröße der Daten und die Zeitabstände, in denen sich der AP im Netzwerk als Router meldet. Bestätigen Sie die Einstellungen abschließend mit einem Klick auf „Apply“ und starten

Sie Ihren Access Point neu. Damit sollten alle Verbindungsprobleme gelöst sein.

Reichweite per WDS erhöhen

Mittlerweile gibt es W-LAN-Funklösungen, die bis zu zwei Kilometern reichen, verspricht zumindest der Hersteller. Allerdings kosten diese Profi-Geräte noch bis zu 1.000 Euro (**www.proxim.com**).

Für alle, die mal nicht kurz das Geld für einen neuen Rechner in die Vernetzung stecken möchten, gibt eine einfache und außerdem relativ günstige Lösung: Wireless Distribution Service (WDS). Über diesen Dienst lassen sich zwei Access Points per Funk miteinander verbinden und damit die Reichweite des Drahtlosnetzwerkes drastisch erhöhen. Besonders bei einem W-LAN in mehrstöckigen Häusern macht sich diese Erweiterung positiv bemerkbar.

CHIP zeigt am Beispiel des Access Points Asus WL500G (**www.asus.com**, 60 Euro), wie es funktioniert. Prinzipiell können Sie natürlich alle WDS-fähigen Geräte zu einem Verbund zusammenschließen.

Öffnen Sie das Konfigurationstool des Asus-Routers im Internet Explorer, indem Sie in der Adresszeile die IP „192.168.1.1“ eingeben. Tippen Sie dann im Menü „Wireless“ auf „Bridge“ und aktivieren Sie unter „AP Mode“ den Wert „Hybrid“; damit verbindet sich der AP zu anderen Access Points und bietet gleichzeitig die Möglichkeit, W-LAN-fähige Geräte anzusprechen. Wenn Sie die beiden Komponenten nur als drahtloses Netzwerkkabel zwischen zwei Rechnern nutzen wollen, geben Sie „WDS only“ ein.

Unter „Channel“ wählen Sie noch einen festen Kanal aus, den die beiden Geräte verwenden sollen. Bei „Connect to APs in Remote Bridge List“ aktivieren Sie „Yes“, unter „Allow anonymous“ setzen Sie den Punkt vor „No“. Jetzt müssen Sie nur noch die Mac-Adresse des anderen Access Points in die untenstehende Liste eintragen. Die Adresse finden Sie auf der Unterseite des Access Points aufgedruckt. Bestätigen die neue Konfiguration abschließend mit einem Klick auf „Finish“ und starten Sie den Router neu. Gehen Sie beim anderen Gerät dann genauso vor.

Fabian von Keudell

WIRELESS DISTRIBUTION SERVICE: Im Konfigurations-Menü Ihres Access Points können Sie diesen mit anderen Access Points in Reichweite zu einem Verbund zusammenschalten.

KNOW-HOW

Die Zukunftstrends bei W-LAN

Eigentlich sollten die Access Points, Router und Netzwerkkarten ja schon heute perfekt miteinander arbeiten können. Doch das ist in vielen Fällen Wunschdenken. Immer wieder kommt es zu Kompatibilitätsproblemen bei den unterschiedlichen Herstellern. Der Grund: Die preiswerten Geräte halten sich nicht hundertprozentig an die festgelegten Standards. Aber auch bei der Verschlüsselung gibt es Probleme: Die unsichere WEP-Codierung verschwindet zwar zunehmend vom Markt, aber auch der Nachfolger WPA wurde schon gehackt. Gerade deshalb gibt es einige Neuentwicklungen, die endlich einen einheitlichen Standard für Sicherheit, Bandbreite und Reichweite für alle festlegen sollen.

WPA-2 Ende 2004 hat die Wi-Fi Alliance begonnen, W-LAN-Geräte zu zertifizieren, die die neue Verschlüsselungsmethode WPA2 (Wi-Fi Protected Access 2) beherrschen. Der Clou: Diese nutzt zur Codierung die AES (Advanced Encryption System)- Methode und wurde bisher noch nicht genackt. WPA2 wird auch Teil des IEEE 802.11i-Standards sein. „Produkte die für WPA2 zertifiziert sind, geben IT-Managern die Gewissheit, dass die Technologie den Standards entspricht, und helfen, Support und Einrichtungskosten zu steuern“, so Franz Hanzlik, Managing Director der Wi-Fi Alliance.

WPA2 ist zwar abwärtskompatibel, kann aber bei vorhandener W-LAN-Hardware zu Problemen führen, insbesondere wenn ältere Komponenten zum Einsatz kommen. Dies liegt an der Verschlüsselungsmethode AES, die wesentlich mehr Prozessorleistung verlangt; die meisten Hardware-Anbieter integrieren daher einen speziellen Prozessor in die neue W-LAN-Hardware, um diese zusätzliche Belastung aufzufangen.

WMM Zusätzlich zum neuen Verschlüsselungsstandard kommt WMM (Wi-fi Multimedia), der den QoS (Quality of Service) Dienst für W-LAN-Router aktiviert. Ohne diesen haben alle Applikationen die gleichen Rechte, um Daten über das Netz zu versenden. Mit Internetbrowsern oder E-Mail-Anwendungen klappt das auch ganz gut; Probleme gibt es erst, wenn Multimedia-Programme dazukommen. Diese haben in speziellen Fällen nicht mehr genügend Übertragungsgeschwindigkeit, um etwa Videos flüssig abzuspielen. WMM konfiguriert das drahtlose Netzwerke so, dass für Multimedia-Anwendungen immer genügend Bandbreite zur Verfügung steht.

Die meisten Geräte lassen sich per Firmware-Update auf den neuen Standard bringen. Für alle anderen kommt WMM mit dem IEEE802.11e-Standard.

MIMO-Antennen Um die Reichweiten der Funknetzwerke zu erhöhen, gibt es verschiedene Ansätze der Hersteller: Die einen bauen empfindlichere Antennen, die anderen bieten Repeater an, die das Signal verstärken. Am erfolgversprechendsten ist allerdings die Entwicklung der MIMO-Antennen (Multiple Input, Multiple Output). Als erstes setzte die Firma Netgear diese Technologie ein und nannte es RangeMax. In den Geräten befinden sich sieben intelligente Antennen, mit denen 127 verschiedene Antennenmuster nachgebildet werden können. Diese ermöglichen die Anpassung an die jeweilige Netzwerkumgebung, indem sie sich an RF-Störungen (Radio Frequency), Positionen der Clients und physikalische Hindernisse anpassen. Hierdurch ergeben sich große Reichweiten sowie unterbrechungsfreie Datenübertragungsgeschwindigkeiten im Bereich des Funknetzwerkes. Die Komponenten kosten um die 100 Euro (www.netgear.de). Voraussetzung für die erweiterte Übertragung sind allerdings RangeMax-Geräte auf beiden Seiten, also eine aktuelle PCI- oder PC-Karte und ein Router.

Tuning fürs Funknetz

W-LAN voll ausreizen

Mit Ihrem Funknetzwerk können Sie viel mehr als nur im Garten surfen. Auch drahtloser Multimedia-Genuss und die kabellose Nutzung von Druckern oder Fileservern lassen sich mit wenig Aufwand realisieren. CHIP zeigt Ihnen die vielfältigen Einsatzmöglichkeiten und hilft Ihnen, Stolperfallen bei der Einrichtung zu vermeiden.

Netzwerk-Leitungen, Strom- und Antennenkabel, DSL-Verbindungen – mittlerweile schlängelt sich ein dicker Strang an Stolperfallen quer durch viele Wohnungen. Computer-affine Anwender steuern nun dagegen: Eine Umfrage auf **www.chip.de** zeigt, dass bereits 35 Prozent der User ein Funknetzwerk nutzen – Kabelchaos ade!

Allerdings: Das Einrichten eines schnurlosen Geräteverbunds ist häufig knifflig. Da will der Router nicht mit der W-LAN-Karte, der Musik-Player versteht sich nicht mit dem Access Point und das TV-Signal aus dem Rechner kommt partout nicht beim Fernseher an.

CHIP erklärt, wie Sie Ihr bestehendes W-LAN ohne diese Probleme erweitern. Wir binden Audio- und Video-Player ein und nutzen Drucker sowie Festplatten von mehreren PCs. Die meisten Anwender verbinden das W-LAN sinnvollerweise per DSL mit dem Internet, von dieser Ausstattung gehen wir deshalb aus. Mehr zum Einrichten von DSL finden Sie auf **www.chip.de** unter dem Web-Code PRAXIS10.

Das Netz-Equipment kommt von Netgear, dem Hersteller, der rund ein Drittel des deutschen W-LAN-Marktes beherrscht. So oder ähnlich funktioniert das Prozedere allerdings auch mit anderen W-LAN-Produkten.

Musik & Video | Multimedia drahtlos

Das brauchen Sie: Router Netgear WGR614 (70 Euro), Pinnacle ShowCenter (210 Euro) oder Netgear Media Player (130 Euro)

Klingt gut: Musik- und Video-Dateien vom PC ins Wohnzimmer – und das drahtlos. CHIP stellt zwei Lösungen vor: das Pinnacle Show Center, das Musik- und Video-Dateien per Funk vom Rechner holt, und den Netgear Media Player MP101. Der kann allerdings nur Musik empfangen.

Achtung: Schauen Sie für beide beschriebenen Lösungen stets erst nach neuer Software und installieren Sie diese vor dem ersten Einschalten des Geräts.

Pinnacle Show Center: Installieren Sie die mitgelieferte Software auf Ihrem PC. Danach holen Sie das 60 MByte große Software-Update (aktuelle Version 1.51) von **www.pinnaclesys.de** – es behebt Bugs und bringt neue Funktionen. Spielen Sie das Update ebenfalls auf.

Drücken Sie am Show Center den Einschaltknopf und bei Erscheinen des Startbildschirms auf dem Fernseher die Taste [B] auf der Fernbedienung. Tragen Sie auf der Registerkarte „WiFi Setup“ die Einstellungen für Ihr Funknetz ein. Überprüfen Sie die Verbindung mit „Check Signal Strength“. Starten Sie das Gerät neu und verbinden Sie sich zum Media-Server, der nach dem Start in der Auswahlliste erscheint. Hat alles geklappt, führt das Show Center ein Firmware-Update durch. Taucht der Server nicht auf, verbinden Sie PC und Show Center temporär mit einem LAN-Kabel und spielen Sie die Firmware ein.

Netgear Media Player MP101: Holen Sie sich die neue Software-Version aus dem Web (**www.netgear.com**) und installieren Sie diese. Danach schalten Sie den Media Player an. Beim ersten Starten durchsucht er die Umgebung nach Funknetzen. Findet der Player ein W-LAN, verlangt er das Kennwort und verbindet sich. Nun führen Sie noch ein Firmware-Update durch mit „Setup | Maintenance | Upgrade“.

Drucker | Jetzt steht er dort, wo er nicht stört

Das brauchen Sie: Router Netgear WGR614 (70 Euro), Netgear-Bridge WGE101 (70 Euro), Netgear-Server PS121 (120 Euro)

Mit Hilfe des W-LAN steht der Drucker endlich dort, wo Sie wollen und nicht unbedingt direkt neben dem Rechner. Über einen Druckserver können Sie per Funk von jedem Rechner oder Laptop aus drucken. Dazu brauchen Sie beispielsweise den Druckserver Netgear PS121 und eine Bridge, etwa die Netgear-Bridge WGE101. Der Server wird per Kabel am Drucker angeschlossen, die Bridge wiederum am Druckserver. Übrigens: Wenn Sie noch keinen Wireless-Router besitzen, sehen Sie sich den Vigor 2900G von DrayTek für rund 230 Euro an. Er hat bereits einen Druckserver eingebaut.

Eine Option: Sie können den Druckserver direkt per Kabel mit dem Router verbinden. So sparen Sie sich die Bridge, müssen den Printer allerdings in der Nähe des Routers aufstellen.

Netgear Print-Server mit Bridge: Installieren Sie die Bridge mit Hilfe des „Smart Navigators“ von der Installations-CD. Danach geht es an den Druckserver. Spielen Sie auf einem PC die Software auf und folgen Sie den Anweisungen. Vergeben Sie einen festen Servernamen, das erleichtert später die Suche. Um von den einzelnen Rechnern auf den Druckserver zuzugreifen, gehen Sie in die Druckersteuerung von Windows über „Start | Drucker und Faxgeräte“ und wählen dort „Drucker hinzufügen“ aus. Im folgenden Dialog klicken Sie auf „Netzwerkdrucker oder

CHIP → DVD-CODE Basics

- → **Netzwerk-Player** Der VideoLan Client erlaubt es Ihnen Musik, Videos und TV von einem Server über das (drahtlose) Netzwerk auf einen anderen Rechner zu streamen.
- → **Media Player im Netz** Mit on2share setzen Fans des Microsoft Media Players 9 und 10 einen Medienserver auf und streamen Sound- und Videodateien über das Netz.

Drucker, der an einen anderen Computer angeschlossen ist“ und beim nächsten Schritt „Drucker suchen“. Markieren Sie den Printer in der Liste und drücken Sie auf „Weiter“. Zuletzt wählen Sie noch den Treiber aus.

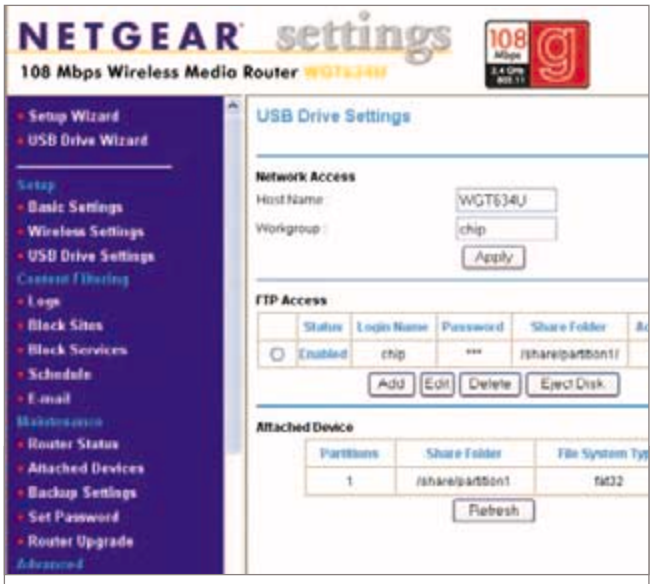
Fileserver | Media-Router mit Datenspeicher

Das brauchen Sie: Router Netgear WGT634U (130 Euro), Maxtor OneTouch 80 GByte (120 Euro)

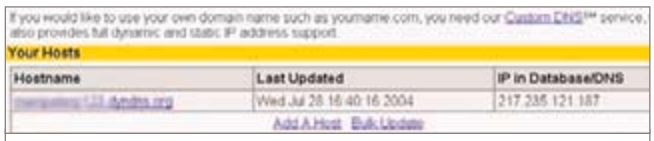
Wenn Sie sich einen PC als Fileserver einrichten, können Sie von jedem anderen Rechner aus auf seinen Datenspeicher zugreifen und Videos, Musikdateien, Dokumente oder andere Dateien herunterladen. Doch die Sache hat einen Haken: Erstens benötigen Sie einen zusätzlichen PC und zweitens macht der nicht nur Lärm, sondern verbraucht auch viel Strom. Die Lösung des Problems ist der Media-Router WGT634U von Netgear für rund 130 Euro. Er ist ideal für diesen Zweck: Ein eingebauter Switch verwaltet die angeschlossenen kabelgebundenen Rechner, der Access Point bietet Wireless-Usern eine 108 MBit/s schnelle Funkverbindung, und der USB-Anschluss dient zum Einbinden von externen Festplatten oder Speichersticks in das Netzwerk. Und so gehen Sie vor:

Installieren Sie den Media-Router wie im Kasten „W-LAN-Router perfekt einrichten“ beschrieben. Spielen Sie danach das Firmware-Update von der Netgear-Site (**www.netgear.com**) ein und starten Sie den Access Point neu. Nun müssen Sie sich entscheiden: Wollen Sie vom internen Netz auf die Platte zugreifen oder über das Internet? CHIP stellt Ihnen beide Wege vor.

Interner Netz-Zugriff: Schließen Sie zunächst die USB-Festplatte an den Router an. Das passende Kabel liegt der Maxtor-Platte bei. Um auf die Freigabe im lokalen Netz zugreifen zu können, müssen Sie eine Arbeitsgruppe einrichten. Gehen Sie dazu zum Punkt „USB Drive Settings“ und tragen Sie unter „Host Name“ den Namen der Gruppe ein, die Sie auch bei allen anderen PCs im Netz eingestellt haben. Bestätigen Sie mit „Apply“. In der Netzwerkumgebung der Clients taucht nun der neue Rechner „WGT634U“ auf. Wenn Sie zweimal darauf klicken, können Sie auf das am Router angeschlossene USB-Gerät zugreifen.



FILESERVER PER W-LAN: Mit Hilfe des Media-Routers Netgear WGT634U geben Sie Ihre Daten im Internet frei.



FILESERVER PER W-LAN: Der Dienst DynDNS weist Ihnen einen Hostnamen zu, über den Sie jederzeit auf Ihre an den Media-Router angeschlossene Festplatte zugreifen können.

Zugriff per Internet: Schließen Sie die externe Festplatte an den USB-Port des Routers an und gehen Sie in das Konfigurationsmenü des Routers. Klicken Sie dort auf „USB Drive Wizard“ und tragen Sie unter „Enter the folder to share“ den Ordner ein, den Sie freigeben wollen, beispielsweise „\programme\dokumente“. Wenn Sie das gesamte Laufwerk freigeben möchten, geben Sie an dieser Stelle „/“ ein. Bestätigen Sie anschließend die Einstellungen mit „Continue“. →

BLITZ-WORKSHOP

W-LAN-Router perfekt einrichten

Am Anfang steht das Grundgerüst in Form des Access Points. Er verwaltet alle W-LAN-Adapter und vermittelt die Daten an die jeweiligen Endgeräte. Damit beim Einrichten nichts schief geht, zeigen wir Ihnen an dieser Stelle, worauf Sie achten müssen.

1 | Der richtige Platz Die Antenne sollte in eingeschossigen Wohnungen immer senkrecht stehen. Wer ein mehrstöckiges Haus versorgen möchte, ist mit einer starken Antenne gut beraten, beispielsweise der ANT2405 von Netgear für rund 45 Euro. Der Access Point selbst sollte nicht vor abschirmenden Hindernissen stehen, also nicht in der hintersten Ecke des Zimmers unter der Couch. Wählen Sie stattdessen für den Access Point einen Platz, der sich ungefähr auf Höhe der Empfangsadapter befindet und möglichst offen liegt. Übrigens: Die meisten Router lassen sich auch an der Wand montieren – ihr futuristisches Design machen sie vielleicht sogar zu einem Hingucker.

2 | Die richtigen Einstellungen Nun müssen Sie Ihren Router nur noch mit dem Netzwerk bekannt machen. Am besten verwenden Sie den Access Point als DHCP-Server (Dynamic Host Configuration Protocol). Damit verwaltet das Gerät sämtliche Zuweisungen von IP-Adressen im Netzwerk ganz automatisch.

Wie das funktioniert, erklären wir am Beispiel des Routers Netgear WGR614:

Verbinden Sie den Router mit Ihrem DSL-Anschluss und den einzelnen Rechnern. Öffnen Sie anschließend an einem beliebigen PC den Internet Explorer und tippen Sie „192.168.0.1“ in die URL ein. Klicken Sie danach auf den Punkt „Setup Wizard“ und folgen Sie den Anweisungen. Damit sind nun die Grundeinstellungen abgeschlossen.

Gehen Sie nun auf die Netgear-Website www.netgear.com und laden Sie von dort die neueste Firmware für den Router herunter. Installieren Sie die Firmware über den Menüpunkt „Router Upgrade“. Damit ist das Gerät auf dem neuesten Stand. Zuletzt nehmen Sie die W-LAN-Einstellungen vor und sichern es mit einer Verschlüsselung wie WEP oder WPA.

Danach tragen Sie unter „Enter the FTP login name of this folder“ einen Benutzernamen ein, mit dem sich die User später am Router authentifizieren können. Klicken Sie anschließend auf „Continue“ und vergeben Sie im folgenden Fenster unter „Enter the FTP login password“ ein Kennwort für die Freigabe; drücken Sie dann wieder auf „Continue“. Nun legen Sie fest, ob der Benutzer nur Leserechte (Read only) oder auch Schreibrechte (Read & Write) bekommen soll. Schließen Sie die Prozedur mit „Continue“ und „Finish“ ab.

Jetzt geht es an die IP-Konfiguration. Bei einem Internet-Provider wie T-Online bekommen Sie bei jeder Einwahl ins Internet eine neue IP zugewiesen und wissen somit nicht, unter welcher Adresse Ihre Festplatte zu finden ist. Auch Nutzer von Flatrates haben dieses Problem, denn die meisten Anbieter trennen die Verbindung nach 24 Stunden und weisen beim nächsten Start eine neue IP-Adresse zu. Mit Hilfe des kostenlosen Dienstes DynDNS können Sie dieses Problem lösen. Dort bekommen Sie einen Internet-Namen im Format **<IhrName>.dyndns.org**, auf den Sie jederzeit zugreifen können. Dieser ist praktisch eine Umleitung auf die aktuelle Adresse Ihres Routers. Der Router selber übermittelt von Zeit zu Zeit automatisch seine IP-Adresse an den Dienst, der damit immer auf dem aktuellen Stand ist.

So geht’s: Navigieren Sie zur Webseite **www.dyndns.org** und legen Sie unter „Sign up now“ einen Account an. Loggen Sie sich anschließend ein und gehen Sie in die Rubrik „Services“. Wählen Sie dort „Dynamic DNS“ und legen Sie mit „Add Host“ einen neuen Internetnamen fest. Tragen Sie dazu unter „Hostname“ einen beliebigen Namen ein und wählen Sie die Sub-Domain „dyndns.org“ aus. Die restlichen Einstellungen lassen Sie unverändert und klicken auf „Add Host“.

Gehen Sie in das Konfigurationsmenü des Routers und klicken Sie auf die Registerkarte „Dynamic DNS“. Aktivieren Sie die Option „Use a Dynamic DNS Service“ und geben Sie unten die Account-Daten von DynDNS ein. Bestätigen Sie abschließend die Einstellungen mit „Apply“.

Fernsehen | Gucken ohne Kabel im Schlepptau

Das brauchen Sie: Router Netgear WGT634U (130 Euro), TV-Karte (ab 50 Euro), VideoLanClient (auf Heft-DVD)

Kabellos Fernsehen, losgelöst von jeder Buchse, klarer Empfang in der ganzen Wohnung – bisher war das nur mit teuren Zusatzgeräten zu haben. CHIP bietet die Freeware-Variante: Alles, was Sie brauchen, ist ein PC mit TV-Karte, der als Server dient, sowie ein W-LAN und einen PC-Client, beispielsweise ein Notebook. So gehen Sie vor:

Server-PC: Starten Sie den VideoLanClient VLC und klicken Sie im Menü „Einstellungen“ auf „Einstellungen“. Gehen Sie zum Punkt „Streamausgaben“ und setzen Sie ein Häkchen vor „Erweiterte Optionen“. Tragen Sie im Punkt „Time To Live“ die Zahl „12“ ein und bestätigen Sie mit „Sichern“ und „OK“. Diese Einstellung garantiert die sichere Übertragung auch bei langsamen Netzen.

Im Hauptfenster klicken Sie nun im Menü „Datei“ auf „Streaming-Wizard“ und wählen im folgenden Dialog „Öffnen“. Klicken Sie auf der Registerkarte „DirectShow“ unter dem Punkt „Bilddevicename“ auf „Refresh list“ und wählen Sie aus der Liste links daneben Ihre TV-Karte aus, etwa „Hauppauge WinTV Capture“. Wiederholen Sie den Vorgang beim Punkt „Tondevicename“ – mit dem Unterschied, dass Sie an dieser Stelle den Toneingang auswählen, in unserem Beispiel „Emu 10Kx Audio [DCC0]“. Aktivieren Sie zum Schluss noch die Option „Device-Eigenschaften“ und bestätigen Sie Ihre Einstellungen mit einem Klick auf „OK“.

Jetzt drücken Sie auf „Wählen“, setzen ein Häkchen vor „UDP“ und geben rechts neben der Adresse die IP des Clients an, auf dem Sie den Videostrom wiedergeben möchten, in unserem Beispiel „192.168.0.3“. Unter „Verkapselungsmethode“ wählen Sie „MPEG TS“. Im Punkt „Umkodierungsoptionen“ wenden Sie sich den Optionen „Bild-Codec“ und „Ton-Codec“ zu. Als Bild-Codec wählen Sie „mp4v“ und als Ton-Codec „mpga“. Hintergrund: Das TV-Signal ist nicht in einen MPEG-Strom gepackt und lässt sich deshalb nicht ohne die Auswahl eines Bild-Codecs auf einem anderen Rechner streamen. Bestätigen Sie anschließend die Einstellungen mit „OK“ und klicken Sie im folgenden Fenster auf „Start“.

Danach wählen Sie unter „Videostandardwerte“ den Punkt „PAL_B“ und bestätigen mit „OK“. Bei den folgenden Einstellungen aktivieren Sie unter „Farbspektrum/-komprimierung“ den Punkt „RGB 32“ und klicken wieder auf „OK“. Im nächsten Schritt wählen Sie unter „Buchsenleiste“ den Punkt „Line-In“ aus und drücken erst auf „Aktivieren“, dann auf „OK“. Die folgenden Meldungen bestätigen Sie ebenfalls mit „OK“.

Client-PC: Auf dem Client – dem Notebook – starten Sie den VideoLanClient und wählen aus dem Menü „Datei“ den Punkt „Netzwerkstream öffnen“ aus. Drücken Sie auf „UDP/RTP“ und tragen Sie danach unter „Port“ die Ziffern „1234“ ein. Mit einem Klick auf „OK“ schließen Sie die Konfiguration ab und starten das Streamen.

Fabian von Keudell

KNOW-HOW

W-LAN-Standards auf einen Blick

Kurz und bündig – CHIP erklärt an dieser Stelle noch einmal die wichtigsten W-LAN-Versionen.
IEEE802.11a: Die 54 MBit/s schnelle a-Version funkt im 5-GHz-Band. Sie darf nur innerhalb von Gebäuden verwendet werden. Der Grund: Auch das Militär nutzt Frequenzen zwischen 5,725 und 5,850 GHz .
IEEE802.11b: Einer der ersten W-LAN-Standards; er schafft nur 11 MBit/s. Die Reichweite liegt bei 25 bis 50 Meter.
IEEE802.11c: Bestimmt, wie Bridges (etwa zur Anbindung eines Druckservers) mit dem Access Point kommunizieren.
IEEE802.11e: Erweiterung für Streaming-Dienste; per QoS (Quality of Service) weist das System den Anwendungen eine festgelegte Datenrate zu.
IEEE802.11f: Beschreibt das Roaming (also den Datenaustausch) mehrerer W-LAN-Zellen, deren Access Points über Bridges verbunden sind.
IEEE802.11g: Die beste Lösung – mit rund 54 MBit/s relativ schnell und mit 25 bis 50 Meter Reichweite auch in größeren Wohnungen gut zu gebrauchen.
IEEE802.11h: Erweitert die a-Variante um die Funktionen „Dynamische Frequenzwahl“ und „Leistungskontrolle“.
IEEE802.11i: Die i-Version ist noch nicht verfügbar. Mit Hilfe dynamischer Schlüsselzuweisung wird sie für mehr Sicherheit sorgen.

Tipps & Troubleshooting

W-LAN im Praxiseinsatz

So faszinierend Wireless-LAN auch ist – ganz ohne Probleme geht's auch bei dieser Technik nicht. Ob Hardware oder Software, überall kann es mal klemmen. CHIP hat für Sie die besten Tipps und Hilfen zur Problemlösung zusammengestellt.

Kennen Sie den Unterschied zwischen „Jeder darf…" und „Alle dürfen…"? Da gibt es eigentlich gar keinen? Windows ist da anderer Ansicht und zeigt sich sehr spitzfindig, wenn es um Freigaben und Ordnerrechte im Netzwerk geht, wie Sie im Tipp 12 nachlesen können. Die wichtigsten Fragen zur schnellen Information über das Thema W-LAN und die besten Troubleshooting-Tipps finden Sie auf diesen Seiten.

TIPP 1 | So schnell ist ein W-LAN wirklich

Nominell soll ein W-LAN nach Standard 802.11b 11 MBit pro Sekunde übertragen. In der Praxis ist dieser Wert aber nicht zu erreichen. Schuld daran sind Störfaktoren wie Strahlungen von Elektrogeräten, Spiegelungen und Wände. In der Praxis sind 5 MBit/s bei fünf Metern Entfernung zum Access Point realistisch, in Ad-hoc-Netzen ist bei gleicher Entfernung meistens nur ein knappes MBit möglich. Die 802.11a- und 802.11g-Netze bringen brutto 54 MBit/s. Praxistests zeigen allerdings: Mehr als 15 bis 20 MBit/s sind einfach nicht drin.

Beim Einsatz von WEP-Verschlüsselung sinkt die Übertragungsgeschwindigkeit bei einigen Routern und Access Points um bis zu zehn Prozent.

Diese Werte unterliegen mehr oder weniger starken Schwankungen je nach Standort; dennoch geben sie ein Gefühl dafür, was mit einem Funknetz in der Praxis möglich ist.

TIPP 2 | So weit funkt ein W-LAN in der Praxis

Die Reichweite ist von der Umgebung abhängig. Hersteller geben 30 bis 50 Meter in Gebäuden und 100 bis 300 Meter im Freien als Maximalreichweiten an. Wände, Bäume und Elektrogeräte verringern diesen Wert.

Beachten Sie außerdem, dass mit wachsender Entfernung die Qualität der Verbindung sinkt – und damit auch die Geschwindigkeit des drahtlosen Netzwerks. Legen Sie den Access Point nicht in die hinterste Ecke unterm Schreibtisch, sondern platzieren Sie ihn lieber oben im Regal, damit er gut in alle Richtungen funken kann.

Auch sollte er nicht direkt auf anderen Geräten liegen – vor allem nicht auf der Mikrowelle. Denn das W-LAN funkt auf der Frequenz, mit der Ihr Essen gewärmt wird. Die Linie zwischen Access Point und Client sollte möglichst auf direktem Weg durch Zwischenwände gehen, also am besten im 90-Grad-Winkel zur Wand. Sonst legen die Funkwellen zu weite Wege durch die abschirmende Wand zurück.

TIPP 3 | Diese W-LAN-Arten gibt es

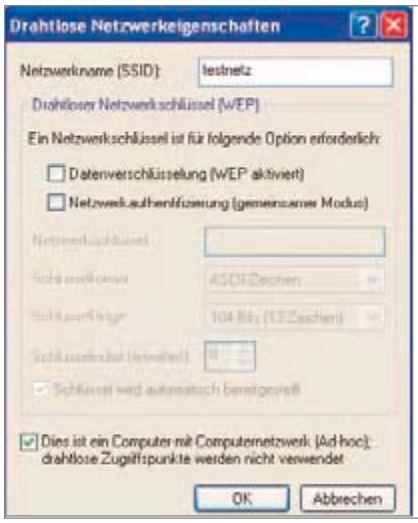
Beim Einrichten der Wireless-Verbindung müssen Sie einstellen, auf welche Art von Netz Sie zugreifen wollen.

Im Ad-hoc-Netz kommunizieren die Rechner direkt miteinander – wie im kabelgebundenen Peer-to-Peer-Netz. Diese billigere Variante ist aber unsicherer, da keine WEP-Verschlüsselung zur Verfügung steht, sie besitzt zudem eine geringere Reichweite. Sie eignet sich aber hervorragend, um beispielsweise spontan im Konferenzraum einige Notebooks zu einem kleinen Netzwerk zusammenzuschließen.

„Infrastructure" bedeutet, dass alle Daten über eine zentrale Basisstation fließen, also einen Access Point. Auch jeder W-LAN-Router enthält einen solchen Access Point, der die Verteilung der Daten an die angebundenen PCs übernimmt. In den meisten Fällen sind Access Points so konfiguriert, dass jedem PC beim Einloggen ins Netz automatisch alle nötigen IP-Adressen mitgeteilt werden.

TIPP 4 | So kompatibel ist W-LAN-Hardware

Solange alle Geräte nach einem einheitlichen Standard arbeiten, sind die W-LAN-Komponenten der unterschiedlichen Herstel-



3 | VERSTECKT: Für Ad-hoc-Netze muss in den Netzwerkeigenschaften der Haken ganz unten gesetzt werden.

CHIP → DVD-CODE Administration

- → **Mehrere Netze verwalten** Auf Heft-DVD finden Sie die Shareware-Version des MultiNetwork Managers, mit dem Sie per Mausklick die Netzwerkkonfiguration ändern.
- → **Freigaben einfach nutzen** Mit dem Gratis-Tool NetConnect verwalten Sie beliebige Freigaben auf entfernten PCs und lassen diesen automatisch Laufwerke zuweisen.

4 | SCHNELLER: D-Links AirPlus-Hardware ist auch zu herkömmlichen Geräten kompatibel. Auch andere Hersteller wie SMC haben 22-MBit-Hardware im Angebot.

5 | PRAKTISCH: Samsung erlaubt in seiner W-LAN-Utility, verschiedene Profile anzulegen. So kann man schnell zwischen mehreren W-LANs hin- und herspringen.

ler „interoperabel". Im Klartext bedeutet das: Sie arbeiten ohne Probleme zusammen. Bei den verschiedenen CHIP-Tests konnten wir keine Schwierigkeiten bei der Kommunikation von W-LAN-Hardware verschiedener Hersteller feststellen.

Auf den Hersteller achten müssen Sie nur, wenn Sie besondere Geräte kaufen, die nach einem proprietären Standard arbeiten, etwa die AirPlus-Reihe von D-Link, deren Modelle 22 MBit/s übertragen können – aber eben nur, wenn auch die Client-Hardware am PC oder Notebook den Standard unterstützt. Auch diese Access Points und Router sind zum 802.11b-Standard kompatibel, können dann aber nicht ihre volle Geschwindigkeit entfalten.

W-LAN-Karten nach 802.11b funktionieren in neuen 802.11g-Netzen ohne Probleme. Die Standards 802.11a und 802.11b sind jedoch nicht kompatibel.

TIPP 5 | Die richtige Windows-Version fürs W-LAN

Besonders einfach ist das Einrichten eines drahtlosen Netzes mit allen Versionen von Windows XP. Das Betriebssystem ist bereits auf die Technik vorbereitet.

Alles, was Sie brauchen, ist ein Treiber, um die W-LAN-Karte zum Laufen zu bringen. Die mitgelieferten Utilities zur Einrichtung und Konfiguration benötigen Sie dagegen nicht, denn das Betriebssystem Windows XP verwaltet ein Wireless-LAN über die Netzwerkverbindungen.

Ganz anders sieht es mit allen übrigen Windows-Versionen aus. Als die entwickelt wurden, steckte W-LAN noch in den Kinderschuhen. Ohne die Utilities der Karten können Sie auch unter Windows 2000 nichts in Betrieb nehmen.

Das ist aber kein Problem, denn die Tools vieler Hersteller bieten ohnehin erheblich mehr Möglichkeiten als die XP-Einstellungen für die „Drahtlose Netzwerkverbindung", beispielsweise das Anlegen von Profilen. Deshalb kann es auch unter Windows XP durchaus sinnvoll sein, die mit der W-LAN-Karte mitgelieferten Utilities einzusetzen.

TIPP 6 | Einen Access Point ins LAN integrieren

In großen Firmennetzen übernimmt ein DHCP-Server die Verteilung von IP-Adressen an die angeschlossenen Clients. Wollen Sie einen Access Point an dieses LAN anschließen, gibt es einen Konflikt, denn auch der Access Point (oder Router) enthält einen DHCP-Server.

Verteilen darf die IP-Adressen aber immer nur einer im Netzwerk, sonst könnten Adressen doppelt vergeben werden und die Kommunikation wäre gestört. Deshalb kann man im Setup der Wireless-Geräte den DHCP-Server abstellen (meist unter dem Punkt „LAN Configuration"). Das sollten Sie unbedingt tun, bevor Sie das lokale Netz mit eigenem DHCP-Server an Ihren Access Point anschließen. Andernfalls bekommen Sie früher oder später Ärger mit Ihrem Netzwerkadministrator.

Bei einigen neuen Routern lässt sich der Adressbereich frei konfigurieren, sodass man ihn auch auf den Adressbereich des eigenen lokalen Netzes einstellen kann. Das kann in Absprache mit dem Netzwerkadministrator geschehen: Er weist Ihnen einfach einen Adressbereich von zum Beispiel 20 Adressen zu, die Sie über ihren Access Point verteilen dürfen.

Arbeitet Ihr Rechner im IP-Adressbereich des Firmennetzes, können Sie in vielen Fällen nicht mehr auf das Web-Interface Ihres Access Point zugreifen. Der ist nämlich meist auf Adressen à la 192.168.x.x eingestellt – Zugriffe aus anderen Adressbereichen erlaubt er nicht.

Wollen Sie etwas an der Konfiguration ändern, müssen Sie die IP-Adresse Ihres Rechners per Hand auf einen Wert im Adressbereich 192.168.x.x einstellen. Den Eintrag für Standardgateway und DNS-Serveradresse können Sie frei lassen. Wichtig sind nur die lokale IP und die Subnetzmaske. Für Letztere nehmen Sie einfach den von Windows automatisch vorgeschlagenen Standard 255.255.x.x.

TIPP 7 | USB-Geräte mit Strom versorgen

Wer mehrere USB-Geräte an einen Port hängt, bekommt unter Umständen Probleme mit der Stromversorgung.

Die meisten USB-Geräte wie Webcams und auch Wireless-USB-Adapter werden über den USB-Port mit Strom versorgt. Standardmäßig liefern USB-Ports 500 Milliampere – ist ein USB-Hub ohne zusätzliche Stromversorgung angeschlossen, teilen sich die angedockten Geräte den zur Verfügung stehenden Strom. Also: Entweder Sie kaufen einen aktiven Hub mit zusätzlicher Stromversorgung oder Sie greifen zu einem (seltenen) USB-Adapter mit eigenem Netzteil. →

TIPP 8 | So funktioniert die MAC-Adressen-Filterung

Jedes Stück Netzwerk-Hardware hat eine so genannte MAC-Adresse – eine Nummer, welche die Hardware weltweit eindeutig identifizieren soll.

Viele Access Points und Router können nach MAC-Adressen der Clients filtern. So können Sie festlegen, welches Gerät Zugang zum Netz bekommen darf und welches nicht. Der Vollständigkeit halber sei noch erwähnt: Auch dies ist kein absoluter Schutz; wenn ein Hacker es darauf anlegt, in Ihr Netz einzudringen, wird ihn das nicht abhalten.

TIPP 9 | Einen PDA ins Wireless-LAN einbinden

Auch Organizer lassen sich problemlos in eine Wireless-Umgebung einbinden. Je nach PDA können sich ein Compact-Flash-Adapter, eine SD-Card oder eine herkömmliche PCMCIA-Karte als beste Variante erweisen.

Einige neue PDAs bieten die W-LAN-Unterstützung gleich von Haus aus. Um Akkuleistung zu sparen, sollten Sie das W-LAN-Modul aber nur einschalten, wenn Sie es wirklich brauchen. Dasselbe gilt für das in einige mobile Geräte integrierte Bluetooth, das mit W-LAN im Übrigen nicht kompatibel ist.

Aufgepasst beim Kauf einer PCMCIA-Karte: Nicht alle Hersteller halten auch Treiber für Pocket-PCs vor. Auf der sicheren Seite sind Sie mit Karten von Markenherstellern: Hewlett-Packard preist seine W-LAN-Karte als ideale Erweiterung für einen iPAQ mit Expansion Slot an.

TIPP 10 | Mehrere LAN-Konfigurationen nutzen

Viele Anwender nehmen ihr Notebook vom Büro mit nach Hause, um dort in ihrem eigenen, lokalen Netz weiterzuarbeiten. Oder sie wollen sich bei Besuchen in einer Firmenfiliale in das dortige Netzwerk einklinken. Arbeitet eins der beiden Netze (oder beide) jedoch mit festen IP-Adressen, ist der Anmeldevorgang recht umständlich. Sie müssen dann jedes Mal zunächst die Netzwerkeinstellungen ändern, bevor Sie Zugriff auf das Netz bekommen.

Um dieses Problem zu lösen, bietet Windows XP eine alternative Netzwerkkonfiguration an. Sie erreichen sie bei den „Eigenschaften“ der „LAN-Verbindung“. Markieren Sie „Internetprotokoll (TCP/ IP)“, rufen Sie die „Eigenschaften“ auf und öffnen Sie das Register „Alternative Konfiguration“.

10 | ZWEITNETZ: In Windows XP lässt sich eine zweite TCP/IP-Konfiguration definieren, etwa um sich mit einem Notebook schnell in ein anderes Netzwerk einloggen zu können.

Arbeitet beispielsweise in der Firma ein DHCP-Server, so stellen Sie zunächst im Register „Allgemein“ ein, dass die IP-Adresse und die DNS-Serveradresse automatisch bezogen werden sollen. Wechseln Sie dann zu „Alternative Konfiguration“ und stellen Sie dort die festen IP-Adressen für das Heimnetzwerk ein. Sobald Sie sich nun daheim bei Ihrem Netz anmelden, sucht Windows zunächst nach einem DHCP-Server. Wenn es keinen findet, verwendet es automatisch die alternativen Einstellungen. Eine wichtige Einschränkung gibt es allerdings: Mit der alternativen Konfiguration lässt sich kein Wechsel zwischen zwei Domänen bewerkstelligen. Und: Diese Funktion ist nur in Windows XP Home und Professional enthalten, in den anderen Windows-Versionen fehlt sie. Dafür gibt es jedoch Tools aus der Shareware, die dem gleichen Zweck dienen. Empfehlenswert ist etwa der MultiNetwork Manager (36 Dollar, **www.globesoft.com/mnm_home.html**), der vor dem Anmeldedialog von Windows erscheint und auf Mausklick eine andere Netzwerkkonfiguration einstellt. Das Programm lässt auch ein Umschalten zwischen mehreren Domänen zu.

TIPP 11 | Langsamen Netzwerk-Start beschleunigen

Seit Einrichten des Netzwerks geht der Windows-Start nur noch quälend langsam vonstatten.

Durch das Laden von Netzwerkprotokoll(en) und Kartentreiber hat Windows beim Start etwas mehr zu tun. Um viel mehr als wenige Sekunden sollte der Start sich aber auch mit LAN nicht verzögern. Sind möglicherweise zu viele (unnötige) Protokolle installiert? Entfernen Sie alle nicht benötigten Dienste und Protokolle in den Netzwerkeinstellungen.

Auch die automatische IP-Adressenvergabe kostet Zeit; vor allem in reinen Peer-to-Peer-Netzen mit Windows 98 oder Me ist dies oft der Grund für Startverzögerungen. In einer solchen Konfiguration werden nämlich – bei Fehlen eines DHCP-Servers im LAN – von Windows alle möglichen Adressen „angepingt“, um noch nicht vergebene IPs zu finden. Je nach Ausbau des Netzwerkes kann das durchaus eine Weile dauern. Weisen Sie zur Beschleunigung des Windows-Starts jedem PC per Hand eine eindeutige IP-Adresse zu.

TIPP 12 | Zugriff auf Serverfreigabe klappt nicht

Für eine Freigabe auf dem Server ist als Standardbenutzer „Jeder“ eingetragen. Trotzdem können Sie nicht auf die Serverfreigabe zugreifen.

Der Eintrag „Jeder“ ist missverständlich, da damit nicht jeder beliebige Anwender gemeint ist. Stattdessen fasst Windows unter dem Gruppennamen „Jeder“ nur die in der Benutzerverwaltung registrierten Benutzer zusammen. Falls Sie also auf eine Freigabe nicht zugreifen können, obwohl „Jeder“ dort Leserechte hat, ist es wahrscheinlich, dass Sie am Server nicht als Benutzer registriert sind.

TIPP 13 | Netzwerkeinstellungen überprüfen

Bei Verbindungsproblemen im Netz sollten Sie grundsätzlich zunächst die Netzwerkeinstellungen von Windows XP überprüfen, um festzustellen, ob das LAN richtig konfiguriert ist.

Klicken Sie mit der rechten Maustaste auf „Netzwerkumgebung“, wählen Sie „Eigenschaften“ und im sich darauf öffnenden Fenster „Netzwerk- und DFÜ-Verbindungen“ wählen Sie mit einem Doppelklick „LAN-Verbindung“. Klicken Sie dann auf „Eigenschaften“.

In der Liste sollten vorhanden sein:
„Client für Microsoft-Netzwerke“,
„Datei- und Druckerfreigabe für Microsoft-Netzwerke“ und mindestens ein Protokoll (z.B. TCP/IP).
Über den Button „Installieren…“ können Sie gegebenenfalls fehlende Komponenten hinzufügen.

Für die TCP/IP-Konfiguration klicken Sie den Protokolleintrag an und wählen „Eigenschaften“. Wie bei Windows 98/Me überprüfen Sie hier IP-Adresse und Subnetzmaske.

Die Daten für Arbeitsgruppenbezeichnung oder Domänenzugehörigkeit finden sich bei Windows 2000/XP über einen Rechtsklick auf „Arbeitsplatz“ und die Wahl von „Eigenschaften“. Die zuständige Registerkarte nennt sich in Windows 2000 „Netzwerkidentifikation“, in Windows XP dagegen schlicht „Computername“. An dieser Stelle finden Sie zwei Buttons zur Festlegung des lokalen Rechnernamens, der Arbeitsgruppe oder Domäne. Der obere Button startet einen Assistenten, der untere eine Dialogbox für die direkte Eingabe der Daten.

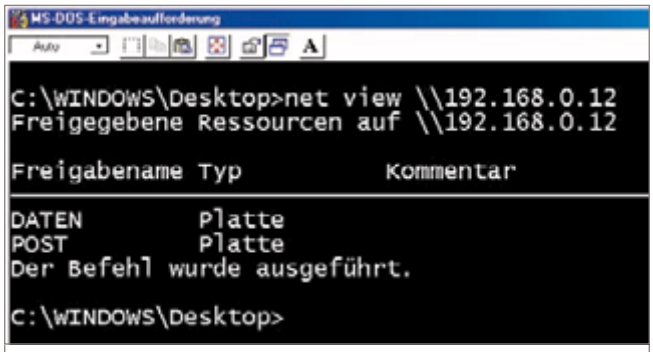
Jetzt haben Sie alle relevanten Punkte der LAN-Installation überprüft. Normalerweise sollte das Netz spätestens nach Abhaken aller Punkte in der Checkliste problemlos laufen. Meist müssen Sie aber gar nicht durch die ganze Liste möglicher Fehlerquellen, sondern können von der Art des Problems schon auf die richtige „lockere Schraube“ schließen.

TIPP 14 | Wenn die Netzwerkumgebung streikt

Häufigstes Problem ist, dass beim Doppelklick auf die Netzwerkumgebung nur ein Icon „Gesamtes Netzwerk“ erscheint. Der Versuch, dieses zu öffnen, führt zur Fehlermeldung „Das Netzwerk kann nicht durchsucht werden…“.

Das ist einer der häufigsten und leider auch komplexesten Fehler bei Windows-Netzwerken. Im Wesentlichen besagt die Fehlermeldung nicht weniger als: „Die Netzwerkkarte funktioniert wohl, ich weiß nur nicht, wo ich bin, ob es überhaupt ein Netzwerk gibt und ob hier noch andere Rechner sind.“

12 | NICHT ALLE: Die Einstellung „Jeder“ steht lediglich für alle registrierten Benutzer des Rechners oder der Domäne, nicht für jeden beliebigen Anwender.



14 | HINTERTÜR: Mit dem Befehl „net view“ und der Adresse eines Netz-PCs erfahren Sie auch bei streikender „Netzwerkumgebung“, welche Ressourcen dort freigegeben sind.

Wenn sich andere Ursachen – etwa fehlende Ressourcen-Freigaben im gesamten Netz oder auf dem betreffenden lokalen PC oder Fehler bei den Protokoll- und Netzwerkeinstellungen (Arbeitsgruppenbezeichnungen, IP-Adressen) sowie physikalische Unterbrechungen – ausschließen lassen, kann der Ausfall des Browse-Masters die Fehlermeldung auslösen.

Hintergrund: Wenn man auf die „Netzwerkumgebung“ klickt, geht es darum zu erfahren, welche Rechner im LAN gerade aktiv sind und welche Ressourcen sie für den Zugriff zur Verfügung stellen. Dabei klappert Ihr lokaler Rechner nicht alle erreichbaren Netz-PCs ab, sondern fragt eine zentrale Datenbank, den Browse-Master. Diese Funktion hat einer der Netzwerk-PCs inne. Dieser wird von allen anderen beim An- und Abmelden und bei der Freigabe oder Sperrung von Ressourcen informiert. Welcher Rechner Browse-Master (BM) „spielt“, wird durch eine interne Wahl der PCs untereinander ausgehandelt und ist nicht einsehbar. Meldet sich der entsprechende Rechner aus dem Netz ab, wird diese Wahl erneut abgehalten.

Falls aber der BM-PC abstürzt oder nicht ordnungsgemäß abgemeldet/heruntergefahren wird, findet keine Neuwahl statt, bis die anderen PCs das merken, was über eine halbe Stunde dauern kann. Wird in der Zwischenzeit die Netzwerkumgebung abgefragt, kann besagte Fehlermeldung auftreten. Sie bedeutet also nur: „Kann Browse-Master nicht finden.“ Das Browse-Master-System ist – zum Beispiel durch den Einsatz von Hilfs-Browse-Mastern in größeren Netzen – noch etwas komplexer.

Sie kommen dennoch ganz ohne Befragen des Browse-Masters an die freigegebenen Netzwerkressourcen. Sie müssen dazu nur deren Namen und Ort kennen oder zumindest die interne IP-Adresse des betreffenden PCs.

Öffnen Sie die Eingabeaufforderung und tippen Sie die Befehlszeile „net view \\<ip-adresse>“, gefolgt von der Eingabetaste. Natürlich ersetzen Sie den Begriff „<ip-adresse>“ durch die richtige Adresse des betreffenden PCs. Es werden dann eventuell freigegebene Ressourcen auf dem betreffenden Rechner mit ihren jeweiligen Namen angezeigt. Alternativ verwenden Sie die Suchfunktion von Windows. Und zwar suchen Sie nach Computern, nicht nach Dateien oder Ordnern. In Windows XP lautet der entsprechende Suchbefehl: „Nach Computern oder Personen suchen“. Den gefundenen PC klicken Sie zweimal an und sehen nun das bekannte Fenster mit den Freigaben.

Florian Schuster, Stefan Wischner

Die nächste CHIP Professionell — Ab 18. April

PC-Security professionell

→ Spam & Mail
Phishing – die neue Bedrohung, Alles über Spam, Hoaxes & E-Mail-Spoofing, E-Mails gekonnt verschlüsseln

→ Viren & Malware
Security-Suiten im Test, Gefahren durch DDoS, Trojaner, Zombie- & Bot-Netze, Web-Hijacker, Firewall perfekt einrichten, Penetrationstest als Sicherheits-Check

→ Spyware & Privacy
Anti-Spyware-Tools im Test, Surf-Spuren vernichten, Überwachungsprogramme im Unternehmen, Cross-Site-Scripting & Script-Missbrauch

→ Special: PC/LAN absichern
Ethernet und W-LAN komplett abschotten, Router richtig sichern, Security-Checks im Internet, alternative Mail-Clients & Browser

IMPRESSUM

Chefredakteur Sonderhefte: Thomas H. Kaspar (verantwortlich für den Inhalt)
Stellvertretender Chefredakteur: Andreas Vogelsang
Redaktion: Niels Held, Fabian von Keudell, Dominik Grau
Schlussredaktion: Dr. Kirsten Broecheler
Autoren dieser Ausgabe: Stefan Bönsch, Andreas Bröhl, Michael Coci, Hans Franzl, Christian Gauer, Martin Goldmann, Dr. Ralf Hinkel, Peter Klau, Bernhard Knaus, Martin Kuppinger, Robert Schoblick, Florian Schuster, Michael Schweizer, Prof. Dr. Axel Sikora, Andreas Vogelsang, Thomas Vosseberg, Stefan Wischner
Produktmanagement CHIP-Sonderhefte: Julia Schuster
Leserservice CHIP-Sonderhefte: sonderhefte@chip.de
Grafische Gestaltung: Steffi Schönberger (Ltg.), Isabella Schillert (CvD)
Titel: Steffi Schönberger
EBV: Jürgen Bisch, Gisela Zach
Bildredaktion: Kersten Weichbrodt (Ltg.) Gertraud Janas-Wenger, Gabi Koller
CHIP-CD/-DVD: Thomas H. Kaspar (Ltg.); Felix Godron (Manager), Alfred Stumpf (Produktion)
Geschäftsführer: Josef Zach
Verlags- und Anzeigenleiter CHIP-Sonderhefte: Jürgen Hiller
Herstellung: Dieter Eichelmann, Verlags-Herstellung, Vogel-Service GmbH, D-97082 Würzburg
Verlag: Vogel Burda Communications GmbH, Poccistraße 11, D-80336 München, Tel. (089) 746 42-0, Fax: (089) 74 60 56-0

Die Inhaber- und Beteiligungsverhältnisse lauten:
Alleinige Gesellschafterin ist die Vogel Burda Holding GmbH mit Sitz in Poccistraße 11, D-80336 München
Anzeigenverkauf: Brigitta und Karl Reinhart, Tei. (089) 46 47 29, Fax: (089) 46 38 15
Zentrale Anzeigenverwaltung und Disposition:
Linda Anders, Tel. (089) 746 42-529, Fax -300
Sabine Maurer, Tel. (089) 746 42-252, Fax -300
E-Mail: anzeigen@chip.de
Vertrieb Einzelverkauf:
Burda Medien Vertriebs GmbH, Arabellastraße 23, D-81925 München
Bereichsleiter Vertrieb:
Achim Frank
Digitale Druckvorlagenherstellung:
Verlags-Service, Vogel Service GmbH, D-97082 Würzburg
Druck: AVD Goldach, CH-9403 Goldach

Nachdruck: © 2005 by Vogel Burda Communications GmbH. Nachdruck nur mit schriftlicher Genehmigung der Redaktion, Christiane Bertsch (E-Mail: cbertsch@vogelburda.com)
Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge übernimmt die Redaktion lediglich die presserechtliche Verantwortung. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit ausdrücklicher schriftlicher Genehmigung des Verlages. Die Redaktion CHIP recherchiert akribisch nach bestem Wissen und Gewissen. Sollte trotzdem eine Veröffentlichung Fehler enthalten, kann hierfür keine Haftung übernommen werden. Sämtliche Veröffentlichungen in CHIP erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes, auch werden Warennamen ohne Gewährleistung einer freien Verwendung benützt.